2003

Attack monitoring and localization in an all-optical network

Tao Wu
Iowa State University

Attack monitoring and localization in an all-optical network

by

Tao Wu

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Computer Engineering

Program of Study Committee:
Arun K. Somani, Major Professor
Ahmed E. Kamal
Manimaran Govindarasu
Doug Jacobson
Yuhong Yang
Byrav Ramamurthy, University of Nebraska, Lincoln

Iowa State University

Ames, Iowa

2003

Graduate College
Iowa State University

This is to certify that the doctoral dissertation of

Tao Wu

has met the dissertation requirements of Iowa State University

Signature was redacted for privacy.

Major Professor

Signature was redacted for privacy.

For the Major Program

DEDICATION

To my parents

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AFF	Attack-Free Flow
AFN	Attack-Free Node
AON	All Optical Network
BERT	Bit Error Rate Tester
DNN	Down-stream Neighbor Node
EDFA	Erbium Doped Fiber Amplifier
FAF	Final Attacked Flow
IF	Innocent Flow
LAN	Local Area Network
MAN	Metropolitan Area Network
OAF	Original Attack Flow
OEO	Optical-to-Electrical-to-Optical
OHM	One-Hop-distance Monitor
OSA	Optical Spectral Analyzer
OTDR	Optical Time Domain Reflectometer
PAN	Primary Attacked Node
QoS	Quality of Service
SAF	Secondary Attacked Flow
SAN	Secondary Attacked Node
SNR	Signal to Noise Ratio
TDM	Time-Division-Multiplexed

WAN	Wide Area Network
WDM	Wavelength-Division-Multiplexed
WSS	Wavelength Selective Switch
UNN	Up-stream Neighbor Node

ABSTRACT

An All-Optical Network (AON) is a network in which data does not undergo optical-to-electrical (O-E) or electrical-to-optical (E-O) conversion within the network. Although AONs are a viable technology for future telecommunication and data networks, little attentions has been devoted to the intrinsic differences between AONs and existing existing electro-optic/electronic networks in issues of security management. Without O-E-O conversion, many security vulnerabilities that do not exist in traditional networks are created. Transparency and non-regeneration features make attack detection and localization difficult. However, it is important to detect and localize an attack connection quickly in a transparent AON.

Among all attack methods, crosstalk attack has the highest damage capabilities. Therefore, we specifically focus on diagnosis of crosstalk attacks in this dissertation. We show that it is possible to effectively reduce the number of monitors while still retaining all diagnostic capabilities. We make the following contributions:

1. We provide a crosstalk attack model and a monitoring model.

2. Based on these models, we prove necessary and sufficient conditions for both, a signle-attack and more than one (i.e., k-crosstalk) attack diagnostic network. The key ideas used in our solution are to employ the status of existing connections along with that of test connections as diagnostic data.

3. We develop efficient monitor placement policies, test connection setup policies, and routing policies for such a network. These conditions lead to efficient k-attack

detection and diagnosis algorithms.

4. Finally, we analyze the performance of these algorithms.

By these conditions and policies, we prove that the concept of a sparse monitor system for monitoring and localizing crosstalk attacks in AON is not only possible, but also feasible.

CHAPTER 1 INTRODUCTION

Computer networks have changed the world dramatically in the last century, and will continue to do so in the near future. Among all existing networks, optical networks are emerging as the predominant transport layer technology for telecom service providers, replacing traditional networks in this role [1, 2, 11, 16, 17, 24, 28]. An All-Optical Network (AON) is a new technology that provides very high bit rates. An AON is a network where the user-network interface is optical and the data does not undergo optical-to-electrical-to-optical (O-E-O) conversion within the network [16, 28]. AONs are attractive because they deliver very high data rates, and support a broad class of applications. The ability to route large amounts of data and access different channels makes AON a very appealing option for providing very high-rate access in WANs, MANs, and even LANs.

1.1 Features of All-Optical Network

All-Optical networks exist in today's research environments in two types: time-division-multiplexed (TDM) networks and wavelength-division-multiplexed (WDM) networks [11]. In this dissertation, we only focus on the AON employing WDM. Fiber bandwidth is divided into optical wavelengths using the WDM method, and each wavelength can support 10Gb/s or higher data rate. Thus, one feature of AONs is the fact that they are typically used to carry extremely high data rates. The very high data rates enabled by all-optical technology have four important security ramifications:

1. Even attacks that are short and infrequent can result in large amounts of data being corrupted or compromised.

2. End users may choose to retain protocols designed for slower traditional networks. While such protocols perform well in the domains for which they were intended, the use of such protocols at very high speeds over long distances will allow effective service denial attacks using different methods.

3. The combination of large physical spans typical of wide-area networks with very high data rates produces high latencies. Such latencies imply that large amounts of data may be beyond the reach of anti-attack measures after an attack has been identified.

4. Transparency is another feature of AON with important implications in matters of security.

1.2 Security Problem of All-Optical Network

Emerging AONs are a viable technology for future telecommunication and data networks, and how to provide a high quality and reliable service for customers is studied in [12, 26, 27, 29, 39]. However, the high data rate feature of AON also brings new attack vulnerability problems and require new counter-measure techniques. Unfortunately, their intrinsic security differences from existing electro-optic and electronic networks have received attention only recently. Security in AONs is an important research area, and it is different from communication and computer security in general. While much of the work in the security area is concentrated on privacy and authentication [9, 14, 25, 32, 38], physical layer security of data in AONs is becoming more and more important [16, 30, 31]. This is because the feature of AONs that requires a new security concept relates primarily to AON physical characteristics.

AONs introduce new physical layer mechanisms that change potential models of attack from those that are well known for traditional electronic networks [3]. AONs are typically used to carry extremely high data rates. Moreover, AONs' transparency characteristic means that data does not undergo optical-to-electrical or electrical-to-optical conversion. Thus, connections in such networks are only amplified, but not regenerated at any intermediate components [27]. This transparency characteristic has many advantages in certain aspects, for example, greater flexibility in switch designing, much higher data rates in wide area networks (WANs), metropolitan area networks (MANs), and local area networks (LANs), etc. However, it also creates many security vulnerabilities that do not exist in traditional networks. In a network with regeneration ability, an anomalous connection will lose its attack capability after passing through an intermediary node, while in a network without regeneration ability, a malicious connection can propagate from its primary source to other nodes without losing its attack capability. Transparency and non-regeneration features make attack detection and localization much more difficult.

Here we describe all possible attack types:

1.2.1 Possible Attacks

Attack upon a network can be broadly categorized into six areas:

1. **Traffic analysis attack:** Based on the observation that the ciphertext length usually reveals the plaintext length, attackers can get valuable information from networks by tapping into fibers. If the attacker can get an index of all the documents from somewhere, he can compare the encrypted lengths of the documents and their request strings to the lengths of the observed request and document. A match in lengths between the lengths of an encrypted document and the observed document as well as the encrypted document request and the observed request

indicates a very likely match between the unencrypted forms of the documents. This attack reveals which documents a client received.

2. **Eavesdropping:** This occurs when an attacker covertly listens in on traffic to get sensitive information. It exploits broadcast packet-switched networks, and is effective and efficient. This attack focuses particularly on user IDs and passwords and is favored by insiders and privileged users looking to expand their privilege. This attack has similar characteristics with traffic analysis: the attacker analyzes the traffic and attempts to degrade its quality in both cases.

3. **Data Delay:** The attacker intercepts the data sent by the user to use it later. AONs are somewhat immune to delay attacks owing to the lack of optical memory, and delay attacks are therefore ignored.

4. **Spoofing:** This attack is defined as acquisition of privilege, capabilities, trust, and anonymity by pretending to be a more privileged or trusted process. This attack includes masquerading and Trojan Horse attacks. It exploits trust, unreliable addresses, and weak authentication. Also, it may exploit sophisticated attack scripts. Mostly, this attack is only used above data link layer. Thus, we don't focus on such attack in this dissertation.

5. **Service Denial:** This attack deprives a user or an organization of the services of a resource that they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programs and files in a computer system. Although usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service

attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money. In AONs, the optical signal may be disrupted by the attackers.

6. **Quality of Service (QoS) Degradation:** The attacker overpowers legitimate optical signals with attack signals and may exploit crosstalk sensitive optical devices. This can be used to degrade or deny services.

Not all these attacks can affect the physical layer. In this dissertation, we only focus on those attacks that can be applied on the physical layer, such as traffic analysis and eavesdropping, service denial, and QoS degradation.

1.3 AON Attack Types

Generally, there are three main differences between an attack and a failure:

1. Attacks may spread to many users and many parts of the network, while a component failure only affects those connections passing through it;

2. Attacks attempt to avoid detection, while failures cannot do that;

3. Rerouting traffic connections using a scheme to tolerate hardware failure cannot solve the problems caused by an attack connection.

Because many AON components are premature [16], relatively high crosstalk between WDM channels within existing components appears to be a particularly important security problem. Crosstalk can be exploited either to tap communications or to perform service disruption by injecting malicious signals into a network. Optical amplifiers under attack by jammers may cease to amplify and thus lead to service disruption. Although many AON components such as fibers and amplifiers also exist in electro-optic networks,

transparency makes their vulnerabilities more important for physical security than in a network with regeneration capability.

AON attacks can be divided into two different types:

1. **Service disruption attack.** It includes service denial attack and QoS degradation attack. Physically, this type of attack includes three different attacks:

   (a) **Fiber Attacks.** Fibers ideally propagate light on different wavelengths with only frequency dependent delay and attenuation, and have very low radiation loss. Under normal operating conditions, there is a negligible radiation of power from the fiber. However, unprotected fiber is very vulnerable against any attacker with physical access (e.g., service is easily disrupted by cutting or bending a fiber).

   (b) **Optical Amplifier Attacks.** Optical amplifiers are critical and necessary components for AONs, and the erbium doped fiber amplifier (EDFA) is commonly used in current optical networks. EDFA consists of an optical fiber having a core doped with the rare-earth element erbium. Light from one or more external semiconductor lasers in either of two pump bands, 980 nm or 1480 nm, is coupled into the fiber, exciting the erbium atoms. Optical signals at wavelengths between about 1530 and 1620 nm entering the fiber stimulate the excited erbium atoms to emit photons at the same wavelength as the incoming signal. This amplifies a weak optical signal to higher power. EDFAs can simultaneously amplify signals over a range of wavelengths, making them compatible with wavelength-division-multiplexed (WDM) systems. However, the nature of EDFA operation in WDM communication links and nodes can lead to a phenomenon known as gain competition, whereby multiple independent WDM wavelengths share a limited pool of available upper-state photons within the fiber. The result is that a stronger user (possibly an attacker)

can deprive a weaker user of photons, thus reducing the weaker user's gain, as shown in Figure 1.1. This gain competition, combined with the fact that fiber has extremely low loss, means that EDFA is susceptible to power jamming from remote locations. In some cases, an attacker can cause service denial to many other users from a legitimate network access point by this way.

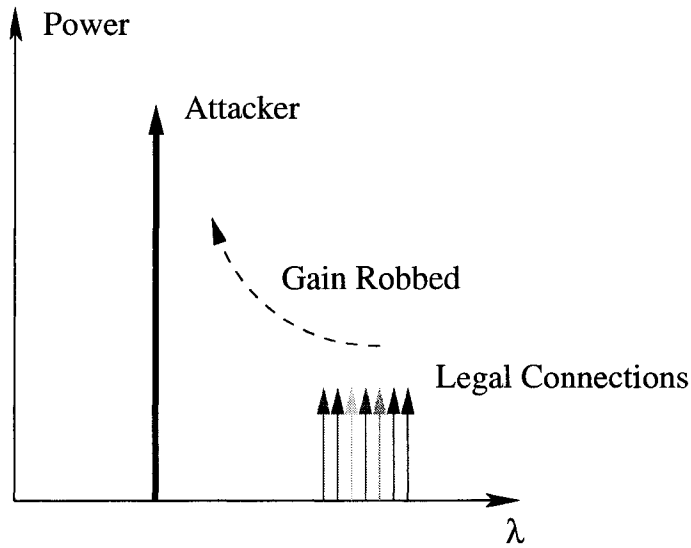


Figure 1.1 Gain competition

(c) **Switching Node Attacks.** Current wavelength selective switches (WSSs) have significant crosstalk levels. Crosstalk causes signals to leak onto unintended outputs and permits inputs to cause interference on other optical signals going through these devices. The level of crosstalk depends greatly upon the particular components and architecture of a switch. In most cases, the leakage of power is only -20dB (e.g., acousto-optical switch) to -30dB (most other switch types) [7, 13]. However, crosstalk is additive and thus the aggregate effect of crosstalk over a whole AON may be much worse than the effect of a single point of crosstalk. An attacker could inject a very strong

signal into the switch. Although only a small fraction of it leaks onto another channel, a sufficiently powerful signal modulated in a malicious way can be highly disruptive, as shown in Figure 2.1. This is the attack that we mainly focus on in this dissertation. We will define such attacks, and carefully model them in Chapter 2 and Chapter 3.

2. **Tapping Attacks.** This attack includes both eavesdropping attacks and traffic analysis attacks. Physically, there are two different attacks in this class.

   (a) **Fiber and EDFA Attacks.** An attacker with physical access to the fiber can retrieve part of a signal with little disruption by slightly bending the fiber. However, at high signal levels (e.g., at the output of an EDFA), fibers exhibit some crosstalk which may be used for tapping by obtaining a position of the signal on the fiber. In EDFA, the gain competition among signals occurs very rapidly, thus tapping can be achieved by observing cross-modulation effects. Also, tapping combined with jamming can lead to service denial attacks (e.g., an attacker can tap a signal and then inject a signal downstream of the tapping point). This is called as correlated jamming, and is shown in Figure 1.2. Such an attack is particularly pernicious compared to the effect of an uncorrelated jamming attack of the same jamming power.

   (b) **Switching Node Attacks.** Because crosstalk signals exist in switches, an attacker can get such crosstalk signals easily by accessing the switch, although the crosstalk signal power is at a low level. Figure 1.3 gives an example of this kind of attack. The attacker's connection, which uses wavelength λ_1, is from host A to host B. The leakage of a normal connection, from host C to host D, is routed onto the bottom fiber. At the same time, the amplifier on this fiber only amplifies signals that are supposed to be on this fiber. Since there is now a connection on the bottom fiber, the amplifier on this fiber still

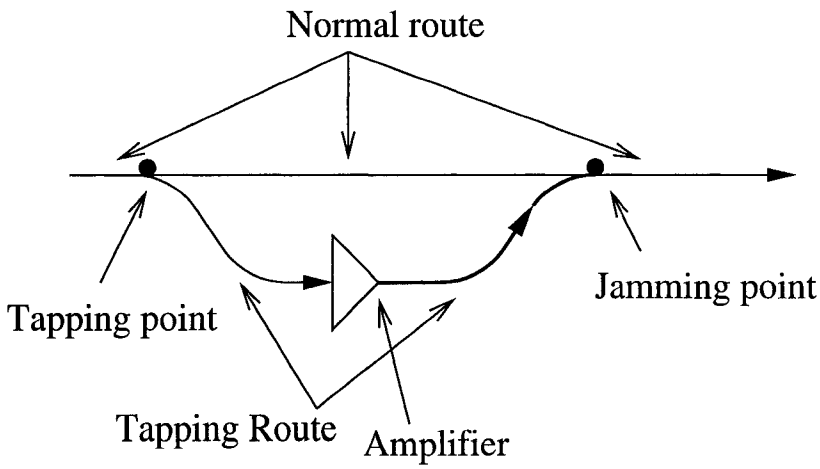


Figure 1.2 Example of a correlated jamming attack

operates. But, if host A does not transmit any power on this fiber, then the only signal on this fiber is the leakage of normal connection from C to D, and host B can easily detect the sensitive call between C and D.

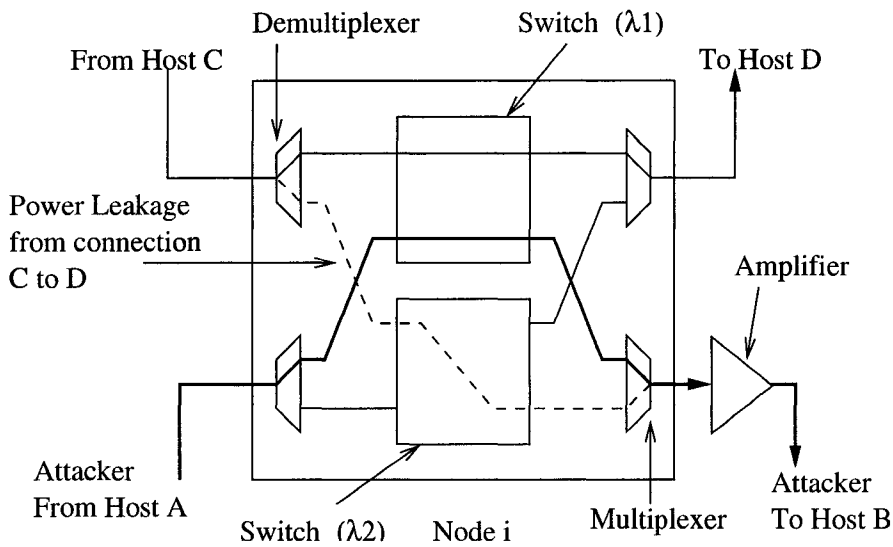


Figure 1.3 Example of tapping attack using switches

1.4 Motivation: Issues in Crosstalk Attack Diagnostic Algorithms

Today's commercial optical networks provide extremely limited attack management. Although optical networking is one of the fastest growing areas in networking, even theoretical attack management research in the optical domain only scratches the surface.

There has been some work [6, 16, 30, 31] in the area of attack localization in AONs, and some detection methods have been proposed. However, these papers do not discuss whether these methods guarantee the localization of every attack connection. If a method cannot guarantee the diagnosis, normal connections incur a risk of being attacked by those undiscovered attack connections. Moreover, these papers assume that all nodes are equipped with monitors.

Other studies [4, 15] describe the capability of an optical monitoring module. Generally, an optical monitor can measure single connection optical power as well as its optical SNR (signal to noise ratio). However, it is expected that such a monitor device will remain expensive in the near future. Therefore, to install a monitor at each node in the network is not an attractive and efficient option.

Some methods [10, 19, 20] develop probabilistic approaches for fault diagnosis in networks. Instead of localizing the exact faulty components, these approaches give the most likely fault set. However, there are some drawbacks of these approaches if we apply them to our attack localization problem. The most important one is that these approaches only give the most likely set instead of determining the exact location of the source. We still need further steps to analyze where the exact location of the source is, and the time consumed by the further analysis may result in a further data loss.

Similarly, the schemes for partially diagnosable systems [36] (some faulty units may not be detected), excess-diagnosable systems [18, 37] (some fault-free units may be incorrectly diagnosed), and sequentially diagnosable systems [34] (assume that multiple

faults do not occur simultaneously, which is not true for attacks) cannot be applied to our problem.

Supervisory connection concepts have also been proposed. A network management system using supervisory connections [21, 22] can detect and monitor the performance of the devices in the network. The advantage of this scheme is that a monitor device can be put in a remote place. The major drawback of such a scheme is that extra supervisory connections are needed to send control signal and detection data. However, this method provides the necessary technique required by sparse monitoring concept.

In the field of system-level diagnosis as applied to a complex multiprocessor system, the diagnosis strategy is to let different processor systems to test each other and identify the faulty units using the test results [35]. Although no system fault detection and location methods can be applied in our problem directly, the testing concept is still helpful. Because a network management system using supervisory connections can detect and monitor the performance of network devices remotely, detecting attack sources is not necessarily equivalent to putting monitors at all nodes. We know that those connections affected by an attack can provide valuable information about the distribution of attack locations. If we can monitor all the connections in the network, we may obtain the necessary information needed for our diagnostic purpose. If normal connections cannot provide sufficient information, we can derive the monitoring information from existing test connections. From previous research [23], we notice that generally the number of idle wavelengths in a network is very large. For example, in a 4×4 mesh-torus network if the connection load of each source-destination pair is 0.3 and the number of wavelengths on each link is 8, then there is more than 70% probability that there will be about 5 idle wavelengths on each link. This information is helpful in establishing a test connection. Moreover, existing connections can also be monitored for malicious attacks. These two together allow us to design an efficient diagnostic system.

Although attack monitoring and localization is important for the security of AON,

unfortunately, neither a clear attack model nor a monitor model has yet been established in previous studies. We seek to close the gap by addressing some of the fundamental research issues and building an attack model as well as a monitor model that could be incorporated in the products as a result of this research effort. Ultimately, we intend to provide quantitative answers to questions about the level of resources needed to support modern attack management system. Our research in attack-diagnostic problem broadly lies in three areas: (i) modeling (i.e., how to model crosstalk attacks); (ii) characterization and algorithms (i.e., how to devise methods for detection and localization of crosstalk attacks); and (iii) policies (i.e., how to implement the various steps involved in the diagnosis of crosstalk attacks).

- **Crosstalk Attack Modeling:** In the area of modeling, our research will be driven by the following issues. How do attack models differ from fault models? How are coordinated attacks best modeled? How can a network measure and detect denial-of-service attacks? In our research, we will build attack models using the physical level characterization performed by others [6, 13, 16, 30, 31].

  To establish clear models for crosstalk attacks and monitor nodes, we study the crosstalk attack special properties and analyze the power levels for attack signals, affected signals, and unaffected signals according to the origination and propagation mechanism for crosstalk attacks. We have observed the difference in the power levels among these signals. According to these difference power levels, we assume different signals have different attack capabilities. With these assumptions, a reasonable crosstalk attack model is established. Furthermore, power-detection based monitoring techniques have also been discussed, and a power-detection monitor model is proposed, too.

- **Characterization and Algorithms:** One problem addressed in this dissertation is whether we can find out the attack source. To locate all co-existing attacks in

an AON simultaneously is another question. To answer these questions, we find out the necessary and sufficient conditions for one-crosstalk-attack diagnosable network and k-crosstalk-attack diagnosable network. Another question addressed in this dissertation is how we can locate the actual attack sources. To solve this problem, we develop a diagnosis algorithm. We define relation matrices and corresponding operations on them to carry out the diagnosis process. We also study the complexities of these algorithms.

- **Sparse Monitoring Policies:** An interesting problem in the attack diagnosis system is whether a sparse monitor network can provide sufficient information for detection and localization purpose. Based on the necessary and sufficient conditions, we develop solutions that only require sparse monitors in the network. It is shown that these solutions are sufficient to detect a single crosstalk-attack. We also develop methods for k-crosstalk-attack diagnosable system. Thus, sparse monitoring concept is not only possible, but is also feasible.

1.5 Contribution and Outline of This Dissertation

The rest of the dissertation is organized as follows. Crosstalk attack is studied in Chapter 2. Its characteristic and attack capability are also described. Based on current available techniques, we study five possible anti-attack mechanisms. We select one, a power detection method for detecting any possible crosstalk attack. Special security requirements for a solution are also presented in this chapter.

An interesting problem in attack diagnosable system is whether a sparse monitor network can provide sufficient information for detection and localization purpose. This problem has been partially studied in [10, 19, 20, 21, 22]. However, these papers do not provide a suitable solution for attack detection, as mentioned earlier. We present a complete crosstalk attack model in Chapter 3, which includes the crosstalk attack

propagation. We also develop a monitor model for the detection purpose in the same chapter according to current available detection techniques while making reasonable assumptions.

Based on these models, a monitor-segment concept is proposed in Chapter 4. We proved a necessary and sufficient condition for a single-crosstalk-attack diagnostic network using this concept. Since in most cases, attackers tend to introduce more than one attack signal into a network simultaneously, localizing more than one co-existing attack signals in an AON is more important in practice. Thus, management of more than one crosstalk attack occurrence in an AON is also studied in the second part of Chapter 4. The question we attempt to answer is what is the necessary and sufficient condition for k-crosstalk-attack diagnostic network. We observe that some of the conclusions that can be made for a single-crosstalk-attack only do not hold for the general case. To solve this problem, we develop a new segment stating monitoring and interpretation model, and extend the single-crosstalk-attack diagnosis condition to k-crosstalk-attack diagnosis condition using the individual monitor-segment status. With these conditions, we can determine whether an attack can be localized or not.

Next we tackle the question of exact location of the attack source. We develop a diagnosis algorithm that is represented as a set of matrix operations to describe the relationship among the monitor-segment status for the existing connections in Chapter 4. By manipulating these matrices, we can accurately locate the attack sources. It is shown that the complexity of these algorithms is $O((|M| \times d_M)^2 \times |C|)$. Here $|M|$ is the total number of monitors in the network, d_M is the maximum degree of all monitor nodes, and $|C|$ is the total number of existing and test connections in the network.

Three sparse monitor placement policies and corresponding routing policies to detect attacks are studied in Chapter 5. Although the two issues are inter-related, the basic idea of our algorithms is that we first determine the monitor placement policy and then design the corresponding routing policy and test connection setup policy.

The first policy requires that all neighbor nodes for a non-monitor node should be monitor nodes. An alternative policy tries to reduce the total number of monitors required in a network. Our policy only requires that one of a non-monitor node's neighbor must be a monitor node. It is shown that both solutions are sufficient for a single-crosstalk-attack diagnostic network. Based on the k-crosstalk diagnosis condition, we propose the third policy for two-crosstalk-attack diagnostic network.

Our solutions do not require that every node be a monitor node. Thus an attack diagnostic network can be a sparse monitor network. Several examples are also presented in the chapter.

The conclusions of our research and directions for future research are presented in Chapter 6.

CHAPTER 2 CROSSTALK ATTACK FEATURES AND MONITORING TECHNIQUES

As mentioned in Chapter 1, there are several kind of attacks that can disturb normal AON communication. Some of these attacks, such as fiber cuts, can be treated as a component failure. Other attacks, like correlated jamming, can only affect those connections that share the same link or the same node with the attack connections.

Among all these attack methods, crosstalk attack has the highest damage capabilities. In this dissertation, we only focus on the crosstalk attack. The attacker injects a malicious signal which has very high power energy, far beyond the expected value. When this connection passes through a wavelength selective switch, the leakage energy (crosstalk) of this malicious connection can be significant and affects the normal connections passing through the same switch. Unlike other attacks, a crosstalk attack can affect not only those connections sharing the same link or node with it, but also may induce attack capabilities to those connections that are attacked [16]. In this chapter, we describe crosstalk attack's origination, its characteristic, and possible anti-attack mechanisms.

2.1 Crosstalk Attack Features

In this section, we explain the origination of crosstalk attack and its features. As shown in Figure 2.1, the crosstalk attack happens at a wavelength switch and only affects the normal connections in the same wavelength. The attacker injects a very

strong signal (the malicious channel shown in Figure 2.1) into a switch, and the power leakage (crosstalk) from the malicious channel is superimposed on a normal channel that shares the same wavelength switch (λ_2 switch). The power of the malicious channel is so high that even its power leakage can still greatly disturb the normal channel. It is possible that the high energy on one wavelength may affect the signal energy on other wavelengths. However, we assume that the probability of such occurrences is low. Therefore, we do not pursue this aspect further in this dissertation.

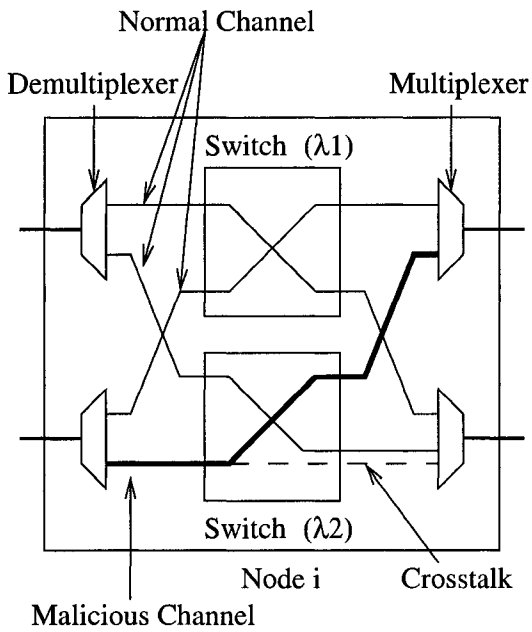


Figure 2.1 Example of crosstalk attack using wavelength selective switches

Besides its attack capability, the crosstalk attack has other features. The most important is its propagation characteristic. Figure 2.2 shows the crosstalk attack propagation mechanism. The original crosstalk attack occurs on node i, which carries connections 1 and 2. Connection 1 is originally a malicious attack connection. Because of the crosstalk attack from connection 1, power of connection 2 is also beyond a certain threshold, so connection 2 itself has crosstalk attack capability. Thus, at node j, which carries con-

nection 2 and connection 3, power leakage from connection 2 also superimposes on connection 3, and connection 3 is also disturbed. This characteristic makes attack connection localization much more difficult. We cannot safely tell whether a connection is a malicious connection based on its attack capability, nor can we locate the source if we only depend on where the attack happens.

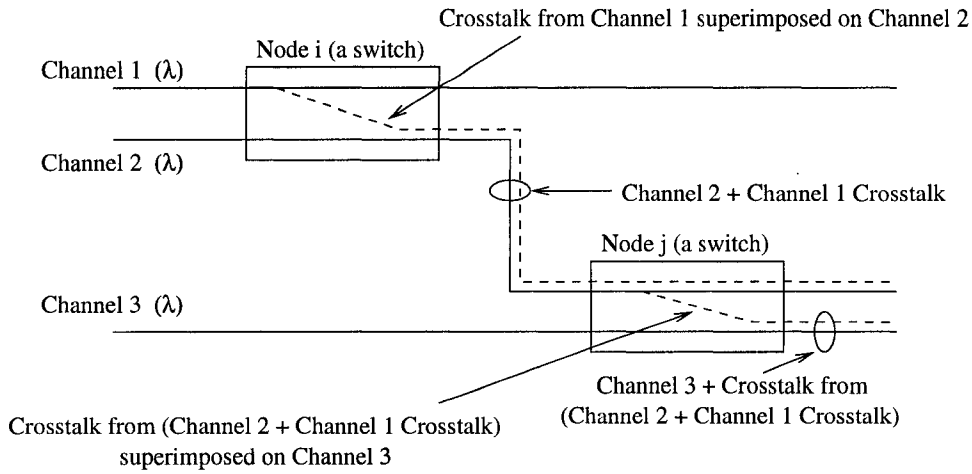


Figure 2.2 Example of crosstalk attack propagation

2.2 Security Consideration

In this dissertation, we discuss AON security requirements. Typically, to solve the security problems associated with AONs, we consider the following issues:

1. **Characterization of security vulnerabilities.** Security vulnerabilities that are specific to AONs stem from the characteristics of the physical devices, such as fiber and amplifiers, which are used in AONs.

2. **Prevention of attacks.** The avoidance of attacks or the judicious design of components and systems to alleviate the security of attacks follows from an un-

derstanding of security vulnerabilities.

3. **Detection of attacks.** Physical security not only requires preventing service disruption and tapping attacks, but also detecting the events where attacks have not been successfully thwarted. Without such detection, it is difficult to launch an appropriate response to attacks.

4. **Localization of attacks.** If an attack is detected but its source cannot be localized, it is difficult to launch an appropriate response. Indeed, the response to an attack whose source is not well identified can lead to consequences which may be more disruptive than the original attack. For example, as shown in Figure 2.2, crosstalk of connection 1 attacks the network by sending an excessively powerful signal. Connection 1 and 2 share the same node i, thus connection 2 also may become too powerful and disturbs connection 3 at node j. Now, both node i and node j may find out the crosstalk attack. Node i may correctly identify the malicious connection as connection 1, while node j may determine connection 2 to be the malicious connection. If the network has no means of localizing the source of the attack, then node i will disconnect connection 1 and node j will disconnect connection 2, which will therefore have been erroneously disconnected.

5. **Response to attacks.** Once an attack has been successfully detected and localized, the network management module can determine the appropriate actions to be taken to thwart or recover from the attack. To do this effectively, an AON network management must be able to differentiate an attack and network traffic problem caused by a physical failure. The strategy for protection and restoration service from hardware failure is simply using a prepared backup path to re-route the disturbed traffic connections from the failure point [5, 8, 33, 45]. However, re-routing traffic connections to tolerate a hardware failure cannot solve the problem caused by an attack. For example, consider that an attack caused by connection 1 on node

i, which has two connections 1 and 2. If the network management treats such an attack as a component failure, then it assumes that node i has failed and reroutes these two connections 1 and 2 to some other node, say j. After this rerouting, node j will appear as having failed because connection 1 will attack other normal connections on node j. The network management system may reroute all these channels to some other node k, and so on. Therefore, it is important for node i under attack to be able to identify an attack coming from its traffic stream and to differentiate it from a physical component failure.

2.3 Overview of Current Monitoring Methods

To detect attack signals, a sophisticated optical monitoring technique is required. With current techniques, we can monitor and detect some important features of an optical signals. Because performance and quality indices of physical optical signals are different, the methods used to measure these indices are variable. Typically, a monitor device should be capable of measuring the following: signal wavelength, signal power, and optical signal-to-noise ratio (SNR). Before we describe these parameters, several testing methods need to be introduced first.

1. **Power detection.** Power detection generally describes the measurement of power over a wide band. Thus it may be used to record an increase or decrease in power with respect to the expected value. Because we are comparing against an expected value, it may take a long time to detect a slight decrease in power. If we use the law of large numbers for statistical analysis, then a very long averaging time may be necessary to establish with reasonable certitude that a deviation of the sample mean from the statistical mean was statistically significant. Some attacks, for instance, a combination of in-band jamming attacks that increase average power

and out-of-band jamming attacks that decrease power might yield no difference in average received power.

The power detection technique is well-suited in some problems such as amplifier failures. It is a basic technique of failure detection in AONs. For an in-band jamming attack, a receiver would receive increased power, and a threshold detector could detect the jamming attack.

The power detection technique, however, is not satisfactory in the detection of gain competition attacks. For gain competition attacks, the received power may not be increased, but rather decreased. Moreover, gain competition attacks can lead to a serious SNR degradation problem without a degradation of total signal power. In these cases, the power detection technique cannot detect the attack at all.

2. **Optical spectral analyzers (OSAs).** OSAs display the spectrum of an optical signal. There are many implementations of OSAs. The main difference between an OSA and a power detector is that the former can provide much more detailed information than the latter, although a bank of specific power detectors can do the same job as one OSA. Thus, they may be able to detect a change of spectrum shape, even if that change in shape does not entail a change in power over the whole channel. However, unless there is significant programming to analyze the output of the OSA and map it to the generation of different types of alarms, it is not a convenient diagnostic tool for the automatic generation of network alarms as is the power detection method. Another drawback is that although OSAs may provide more information than power detectors, they still rely on statistical comparisons between sample averages and statistical averages. Arguments based on the law of large numbers will still imply that infrequent degradations of the signal will not be detected or will be detected only after a long time.

   OSAs can detect those jamming attacks that seriously affect the optical spectrum.

For detecting a gain competition attack, OSAs can determine the attack wavelength by analyzing the signal spectrum.

3. **Bit error rate testers (BERTs):** BERTs operate by comparing a received pattern with the pattern which was known to have been sent. Given the number of discrepancies which are found, the BER of the transmission is estimated. The time it takes for a BERT to establish the BER will depend on the BER and the data rate. For instance, at 1 Gbps, it takes several seconds for a BERT to establish with good statistical accuracy that the BER has been degraded from 10^{-8} to 10^{-3}.

   Another drawback of BERTs is that they only examine a given test data sequence when this special sequence is transmitted. They do not test the actual data. Therefore, an attack can escape detection for a long time until this attack affects a test sequence. Third problem with the BERT is that only data errors can be detected by a BERT. Although most attack forms result in signal BER degradation, some of the attacks may not affect BER seriously.

4. **Pilot tones:** Pilot tones are signals which travel along the same links and nodes as the communication payload, but are distinguishable from the communication payload. Pilot tones are often at different carrier frequencies than the transmitted signal, but they might also be distinguished from the communication payload by certain time slots or certain codes. Their purpose is to detect transmission disruptions. If the pilot tones are present, in frequency, in the close vicinity of the communication transmissions, they are usually referred to as subcarrier multiplexed signals that allow the transmission of network signaling or of a pilot tone at the same carrier wavelength as the payload signal. The tone may be something other than a static tone. The pilot tone may be at a lower or a higher frequency than the communication signal.

   The pilot tone technique may not generate an alarm if an attack at a certain

wavelength does not affect those carrier wavelengths at which the pilot tones are carried. Thus, pilot tones are not effective in detecting jamming attacks unless applied to all wavelengths. Moreover, pilot tones themselves can be masked by malicious signals.

Gain competition attacks affect all wavelengths traversing an amplifier. If the pilot signals are amplified by the same amplifier as the common signals, then the pilot signals can also be affected by such an attack. Otherwise, if the pilot signals are amplified separately, then they cannot detect gain competition attack. In some cases, the pilot tone technique is not used in detecting gain competition attack because such a technique requires detecting a signal at very low SNR levels if the signal suffers from some attack or component failure problem. Thus, although the pilot tone technique can be efficient in detecting link failure or fiber cut problems, it may not be sensitive enough to detect gain competition attack. Moreover, if auto-gain-control devices are applied in networks, then the power of pilot tone can actually be sufficient to mask the occurrence of gain competition attack.

5. **Optical time domain reflectometers (OTDRs):** OTDRs are a special application of pilot tones. Rather than analyzing a pilot tone at the point where the communication signal is received, the pilot tone's echo is analyzed. OTDRs are generally used to diagnose faults, bends, and losses in fibers. Thus, they are usually better adapted to detecting attacks which involve tampering. However, since they operate by reflecting a signal back through the fiber, they may also provide information about other attacks that must be taking place. Note that the signal used for reflectometry may also be used as a supervisory signal, and therefore may share the uses discussed in previous parts. The probe signal may also, for certain unmodulated or very simply modulated probe signals, be subject to jamming in the same way as pilot tones.

By applying OTDRs, jamming attack signals can be returned in the reflections and observed. OTDRs use different diagnostic techniques than pilot tones. If the OTDR probe signal is modulated, then it is very easy to detect the jamming signal super-imposed on the OTDR probe signal. The drawback is that OTDRs cannot detect jamming attacks which occur outside the band of the probe signal or jamming signals which do not affect the probe signal seriously because of simple or non-modulation on the probe signal.

The detection efficiency for gain competition is dependent on the amplifier structure. If the amplifier is unidirectional and there is no preamplifier for the OTDR probe signal, then it cannot be used to amplify the reflected signals. Therefore, OTDRs cannot be used to detect gain competition attack in such networks. Thus, bi-directional amplifiers are required for OTDRs. Moreover, preamplifiers for OTDRs are also necessary. If these conditions are met, the the gain competition attack at the amplifier can be detectable over the reflected OTDR probe signal.

To detect crosstalk attack, we at least need to know the optical signal power value. Also, we hope to establish an effective method of detection that is as simple as possible. Most detection techniques discussed above are too complex, although they may be efficient for some special attacks. However, the power detection technique is good enough to detect the power value of optical signals, and it is the simplest method among all five possible detection techniques. Thus, the power detection technique is selected as the major part in our monitor model, which will be described in Chapter 3.

CHAPTER 3 ATTACK MODEL, NODE MODEL, AND MONITOR MODEL

As mentioned earlier, although attack monitoring and localization is important for the security of an AON, unfortunately, neither a clear attack model nor a monitor model has yet been established. In order to develop a crosstalk attack detection and localization method, we first establish a node model, a crosstalk model, and a monitoring model based on current techniques and reasonable assumptions.

3.1 Node Model

The node is the first important component worthy of discussion, because a crosstalk attack can only take place on nodes, not in any other components, such as fibers or amplifiers. We assume that every node in our network has the following characteristics:

1. The node can perform routing and switching. Without the switching capability, the node cannot propagate a crosstalk attack to other normal connections. In such a case, the node need not be considered as a potential attack propagation node.

2. Some nodes can support monitoring capability as will be described latter. We call a node supporting monitoring capability as a *monitor node* and a node without this capability as a *non-monitor node.*

3.2 Crosstalk Attack Model

As shown in Figure 2.1, the crosstalk attack connection only affects the same wavelength connections. The following terms describe our crosstalk attack model:

1. *Up-stream* and *down-stream neighbor nodes*: For a certain node on a certain connection path, its *up-stream neighbor node* (**UNN**) is the previous node on that path. Similarly, its *down-stream neighbor node* (**DNN**) is the next node on that path. In the rest of this dissertation, $UNN(node\ A,\ connection\ C)$ denotes the UNN of node A on connection C. Similarly, $DNN(node\ A,\ connection\ C)$ denotes the DNN of node A on connection C. Figure 3.1 illustrates two connections c_1 and c_2. For connection c_1, node n is node m's up-stream node, while node m is down-stream node of node n (i.e., $DNN(n, c_1) = m$ and $UNN(m, c_1) = n$). For connection c_2, node n is node m's down-stream node, while node m is up-stream node of node n (i.e., $UNN(n, c_2) = m$ and $DNN(m, c_2) = n$).

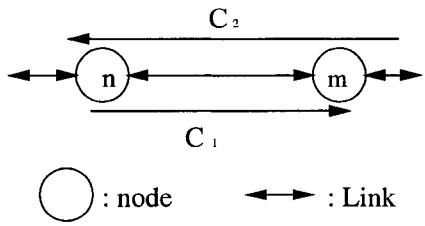


Figure 3.1 Example of up-stream and down-stream neighbor node

2. According to our crosstalk attack concept, there are different types of connections. We explain them separately.

   (a) The *original attack flow* (**OAF**) has a much higher energy level than permitted on a normal connection. The leakage of energy at a switch from the attack connection influences all other normal connections using the same wavelength

on other fibers. The ability of an OAF to influence normal connections is same on its path. A node is called a *primary attacked node* (**PAN**) if there is an OAF originating at, terminating at or passing through this node.

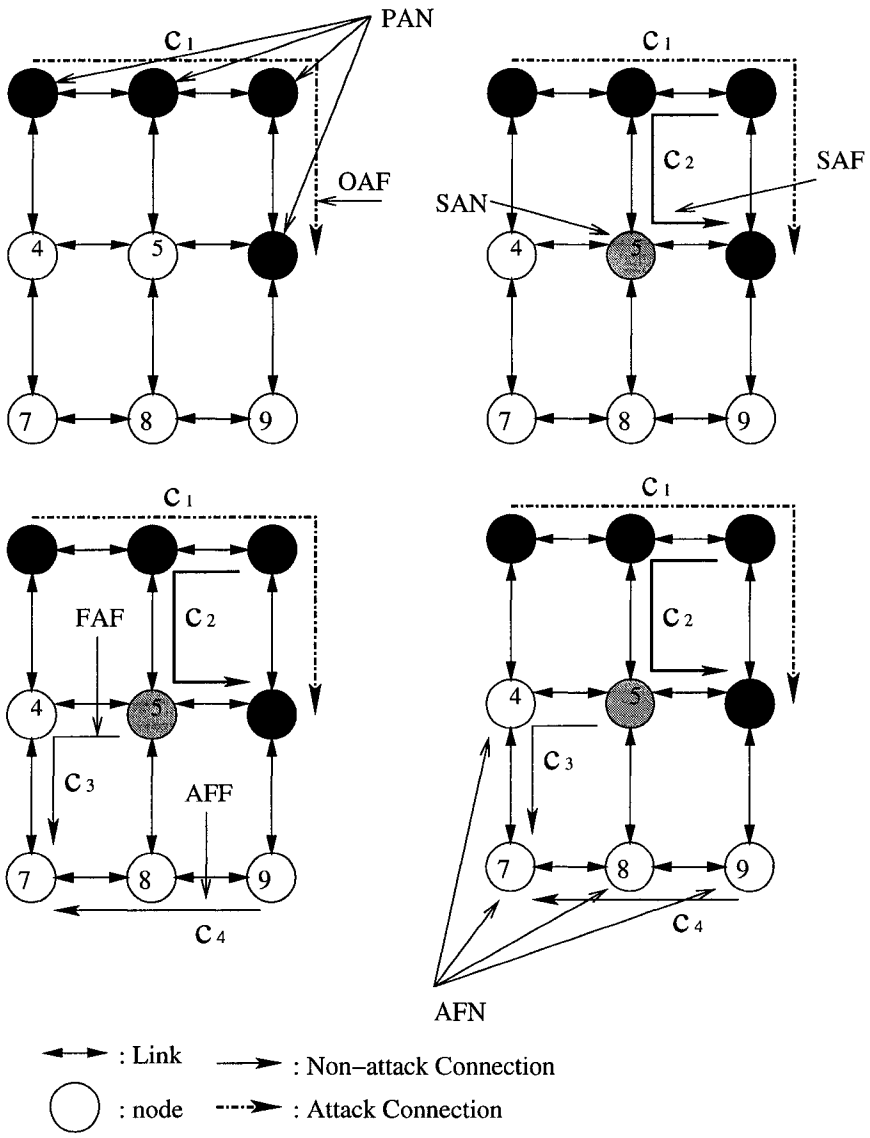


Figure 3.2 Example of attack flow and affected flow

(b) A normal connection sharing a node with the OAF is affected, and this connection is called a *secondary attacked flow* (**SAF**). The SAF has limited attack capability. That is, if a normal connection C gets affected by an OAF at node

u, then the connection C has attack capability only at node $DNN(u, C)$, and we call $DNN(u, C)$ a *secondary attacked node* (**SAN**).

(c) A normal connection influenced by an SAF is called a *final attacked flow* (**FAF**). The FAF does not have the attack propagation capability.

(d) A connection not affected by either OAF or SAF is called an *attack-free flow* (**AFF**). Similarly, a node that is neither a PAN nor a SAN is called an *attack-free node* (**AFN**). The union of AFF, SAF, and FAF is called an *innocent flow* (**IF**) set.

As shown in Figure 3.2, connection C_1 is the OAF, connection C_2 is the SAF, connection C_3 is the FAF, and connection C_4 is AFF. Nodes 1, 2, 3, and 6 are PANs. Node 5 is SAN. The rest, nodes 4, 7, 8, and 9, are AFNs. Connection C_1 can propagate its attack to connection C_3 by affecting connection C_2. According to this, it is expected that the OAF pollutes any connections passing through the PAN, and the SAF pollutes any normal connection passing through a SAN. Connections C_2, C_3, and C_4 are IFs.

3. Since the OAF, the SAF and the FAF have different attack capabilities, it is obviously expected that the power level of these connection channels is as follows:

$$P(OAF) >> P(SAF) > P(FAF) > P(AFF).$$

$P(OAF)$ means the power level of OAF, etc. For example, as shown in Figure 3.2, $P(C_1) > P(C_2) > P(C_3) > P(C_4)$.

3.3 Monitor Node Model

We call a node equipped with a monitor device a monitor node, or a monitor. A node without a monitor device is called a non-monitor node. A monitor needs to be as

simple and cheap as possible. Because crosstalk attacks only change the optical power of normal signals, we only need the crosstalk detection method to detect the change in signal power; more than that seems unnecessary. According to Chapter 2, detection of power levels is simple and meets our detection purpose. Thus, we select power detection method as our core technique in the monitor node model. We describe the model in more detail below.

1. A monitor node can monitor all traffic passing through it, including the traffic that originates/terminates at the node.

2. The monitor node can detect the input/output connection power in all parts, including its demultiplexer, multiplexer, and switch plane, to see if any power level is beyond the expected value. In special cases, when more than one connection's power levels are beyond the threshold, our monitor model can treat these cases in three different ways, as described in bullet 1. We also use power detection methods to monitor the input and output connection signal power levels, as described in Chapter 2, and to monitor separate wavelengths in the input and output fibers. The crosstalk attack monitoring mechanism for selective wavelength switches is shown in Figure 3.3.

3. If a connection in a state of high power traverses a monitor, then we say that this connection is in *attack-status* at that monitor. A connection can be in an attack/non-attack status at a monitor. We use $A/\bar{A}$ to indicate the attack/non-attack status of the connection.

4. One interesting problem is that if there are at least two connections which have attack capabilities passing through a same monitor, how does the monitor identify the difference. Here we give three possibilities and the corresponding three responses from a monitor respectively:

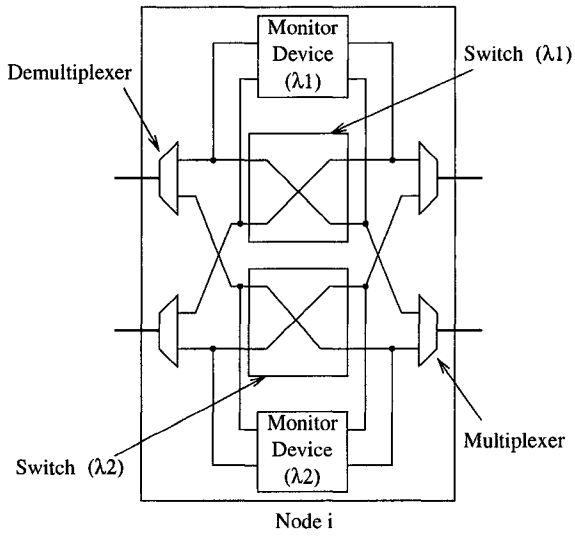


Figure 3.3 Attack monitoring mechanism for selective wavelength switches

(a) One connection is an OAF while all the others are SAFs. Because $P(OAF) > P(SAF)$, the monitor node can detect that one connection has higher power than others do, and the monitor considers only this connection (OAF) to have attack capability. Thus, we assume that only the OAF will be set A, while the other SAFs will be set $\bar{A}$.

(b) More than one connection is a SAF, but none is an OAF. In this situation, the monitor can detect several connections which have similar unexpected high power. We assume that this monitor sets all SAFs to A.

(c) Two or more connections are OAFs. In this situation, similar to the above assumption, the monitor can detect several connections which have similar unexpected high power and set all these connections to A and other connections to $\bar{A}$.

Figure 3.4 shows a 3×3 mesh network. Connection C_1 and C_6 are two OAFs. Node 2, 4, 6, and 8 are monitors. On node 2, because connection C_1 and C_6

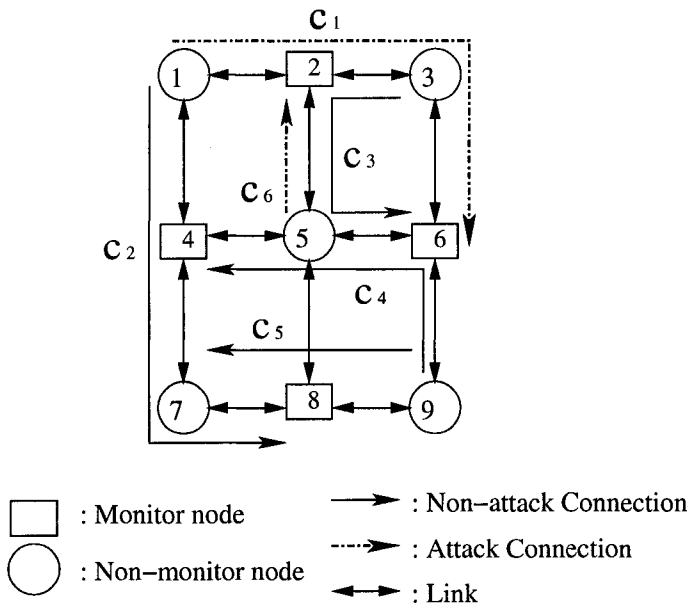


Figure 3.4 Different attack connections passing through monitors

are two OAFs passing through this monitor, connection C_1's status and C_6's status will be set as A, while connection C_3 will be set as $\bar{A}$ because it is SAF. On node 4, both connection C_2 and C_4 are SAFs, and no OAF passes through node 4. Thus, node 4 will set both C_2 and C_4 as A. On node 6, OAF connection C_1 will be set as A while C_3 and C_4 will be set as $\bar{A}$. On node 8, because C_2 does not have attack capability on this node, both C_2 and C_5 will be set as $\bar{A}$.

CHAPTER 4 NECESSARY AND SUFFICIENT CONDITION FOR CROSSTALK ATTACK

In previous chapters, we introduced the AON security problem and crosstalk attack features. Moreover, we proposed a node model, a crosstalk attack model, and a monitor model. As discussed in chapter 3, it is possible to use sparse monitors to create a crosstalk diagnostic network management system. In this chapter, we analyze this possibility and propose some practical methods to create such system based on our analysis. Before we develop an algorithm, we prove that we can always localize all crosstalk attacks in an AON with sparse monitors. First, we only focus on a special situation where only one crosstalk attack exists on each wavelength in whole network. Later on we extend this result to a general case where more than one crosstalk attack exists on each wavelength.

4.1 Necessary and Sufficient Condition for Single Crosstalk Attack in the Network

A network is called one-OAF diagnosable if a single OAF can be always detected and localized from all present connections. In this section we discuss the necessary and sufficient condition for one-OAF diagnosable network.

For a given graph $G(V, E)$, let M denote the set of monitor nodes, and let N denote the set of non-monitor nodes, $M \subseteq V$, $N \subset V$, and $M \bigcup N = V$.

On this graph $G(V, E)$, several connections are established. Let $C = R \bigcup T$ denote the set of connections in the network, where R is the regular set of connections, and T

is the set of test connections.

Let c_i be a connection consisting of nodes $\{u_0, u_1, u_2, \ldots, u_k, \ldots\}$. Let $U(c_i)$ denote the set of nodes on connection c_i's path. Then, c_{ij} denotes a one-hop segment $(u_j \rightarrow u_{j+1})$ on connection c_i.

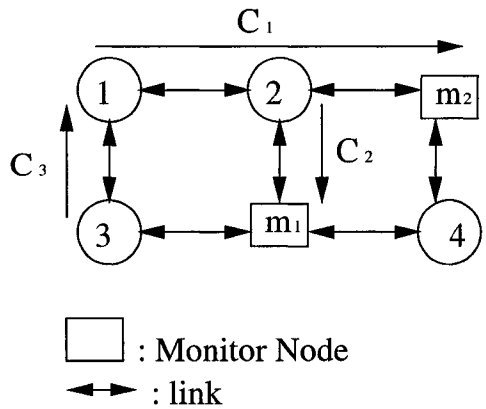


Figure 4.1 Relation between a monitor and a connection

There can be three kind of relations between a monitor and a connection:

1. *Direct-Monitor*: A monitor m is a direct-monitor of a connection c if $m \in U(c)$; for example, as shown in Figure 4.1, monitor m_2 is a direct-monitor of connection c_1 because m_2 is on connection c_1's path: $m_2 \in U(c_1)$.

2. *One-Hop Monitor*: A monitor m is a one-hop monitor of a connection c if $m \notin U(c)$ and $\exists\ (u \rightarrow m)$ where $u \in U(c)$; for example, as shown in Figure 4.1, monitor m_1 is a one-hop monitor of connection c_1 because m_2 is not on connection c_1's path: $m_1 \notin U(c_1)$, and $\exists\ (2 \rightarrow m_1) \subseteq$ connection c_2 where node $2 \in U(c_1)$.

3. *Non-Monitor*: A monitor m is a non-monitor of a connection c if $m \notin U(c)$ and $\nexists\ (u \rightarrow m)$ where $u \in U(c)$. For example, as shown in Figure 4.1, both monitors m_1 and m_2 are non-monitors of connection c_3, because $m_1, m_2 \notin U(c_3)$ and $\nexists\ (u \rightarrow m_1\ or\ m_2)$ in any exist connection where $u \in U(c_3)$.

4.1.1 Monitor-Segment

Monitor-Segment: A monitor segment msc_{ij} is a one-hop segment c_{ij} when node u_{j+1} is a monitor. Let MSC denote the set of the monitor-segments. Let msc_{ij} denote this particular monitor segment. Mostly, we use msc to denote a common monitor segment. Two monitor segments are shown in Figure 4.2, one is made by connection c_2 and monitor node m_1, denoted by m_1c_2, while the other is made by a one-hop segment on connection c_1, from node 2 to node m_2, and monitor node m_2, denoted by m_2c_1.

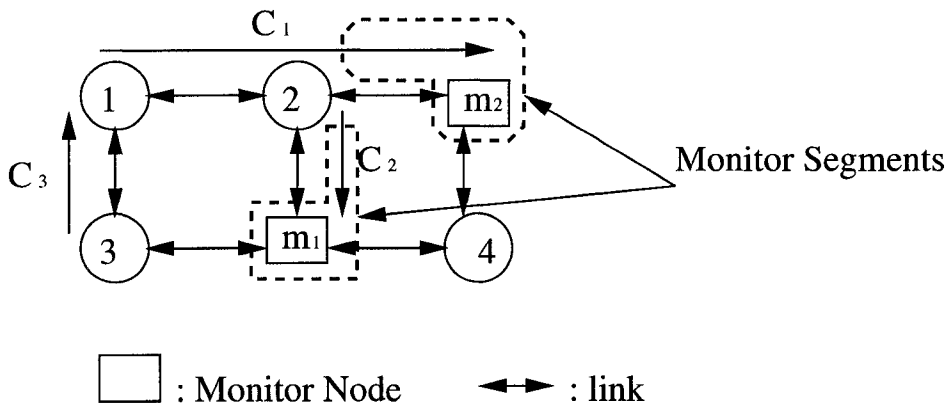


Figure 4.2 Attack monitoring mechanism and Monitor-Segment

A monitor segment $msc = (u \rightarrow m)$ is monitoring a connection c :

1. if the monitor m is a *direct-monitor* of this connection, while the segment $(u \rightarrow m) \in c$, or

2. if the monitor m is a *one-hop monitor* of a connection c, where $u \in U(c)$, and $m \notin U(c)$.

For example, in Figure 4.2, monitor m_2 is a direct-monitor for connection c_1, and monitor m_1 is a one-hop monitor for connection c_1. According to our definition, both monitor segments m_1c_2 and m_2c_1 are monitoring connection c_1, and none of them is monitoring connection c_3. Let (msc, c) denote this relation between monitor-segment

msc and connection c. Consequently, the status of the segment $(u \rightarrow m)$ indicated by monitor m is the *status of the monitor-segment*, denoted by $S(msc)$. For example, in Figure 4.2, if the status of c_2 in monitor m_1 is indicated as A, then the status of the monitor-segment m_1c_2 is A. $S(msc)$ can be either A or $\bar{A}$.

The *status of a connection* can be either innocent flow (IF) or *uncertain*. IF means that the connection is determined as IF, and *uncertain* means that the connection cannot be determined either as IF or as OAF. Let $S(c)$ denote the status of connection c. Table 4.1 shows the relations between a monitor-segment status and its monitoring connection's status.

Table 4.1 Truth Table for monitor-segment and its monitoring/non-monitoring connections

Relation	$S(msc)$	$S(c)$
msc monitoring c	A	*uncertain*
(msc, c)	$\bar{A}$	IF
msc non-monitoring c	A	IF
	$\bar{A}$	*uncertain*

For a connection c, which is not being monitored by msc, we say that msc has $non - monitoring$ relation with c. Table 4.1 shows the relations between a monitor-segment and its non-monitoring connection.

Figure 4.3 depicts two special cases of monitor-segments.

Figure 4.3(1) shows the monitor m as the originating node of the connection c. For this case, monitor m and connection c make up a special monitor-segment msc, and only connection c is monitored by this monitor-segment, while all other connections are not monitored. If $S(msc) = A$, all other connections can be identified as IF.

Figure 4.3(2) shows the relation between a monitor segment msc_1 and a connection

c_2, where $c_1 \notin c_2$, and $n, m \in U(c_2)$. In this case, both c_1 and c_2 share the same nodes n and m. While it seems that c_2 is monitored by msc_1, in fact the relation between connection c_2 and the monitor-segment msc_1 is *non-monitoring*. We can explain it in two ways. First, according to our definition of *monitoring*, the only two cases of monitoring are either the segment is a part of the monitored connection, or the monitored connection does not pass through the monitor. The example provided by Figure 4.3(2) does not fit either of these definitions. Second, according to truth table, suppose the status of msc_1 is $\bar{A}$. We cannot be sure if c_2 is IF or not. According to Table 4.1, this is a *non-monitor* relation.

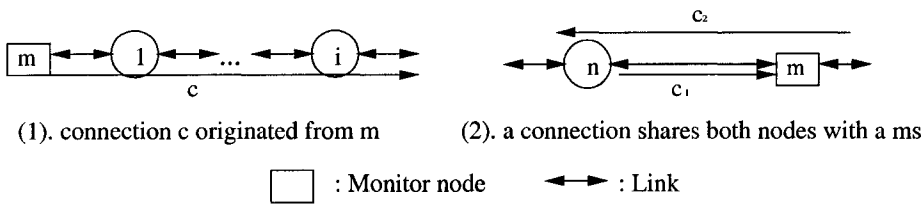


Figure 4.3 Special Monitor-Segment

We can represent the connections and monitors in graph $G(V, E)$, as shown in Figure 4.4(1), using a bipartite graph $G'(V', E')$, as shown in Figure 4.4(3), by using the connections set up in the network. Figure 4.4(2) shows a graph with all connections separated into one-hop segments. For example, c_{1-1} is the first segment of connection c_1 shown in Figure 4.4(1). In graph $G'(V', E')$, the vertices set $V' = \{mc_{ij}\} \bigcup \{C_k\}$ consist of the monitor-segments and the connection (i.e., $mc_{ij} \in MC$), and $c_k \in C$. For example, $3c_{12}$ is a monitor-segment made up by monitor node 3 and one-hop segment c_{12} shown in Figure 4.4(2). An edge in G' depicts a relation between a monitor segment and a connection. In this figure, a directed edge from a monitor-segment msc to a connection c describes the monitoring relation between this pair of monitor-segment and connection, and (msc, c) denotes the edge.

Let $\Gamma(msc_i) = \{c_j | (msc_i, c_j) \in E'\}$ denote the set of connections monitored by a

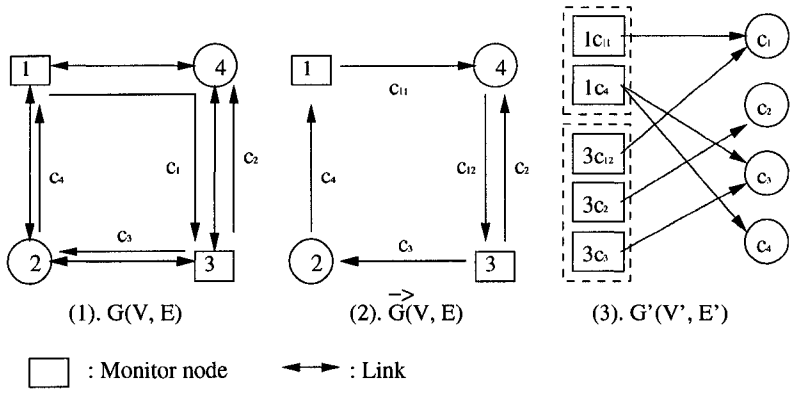


Figure 4.4 Monitor-Segment Example

monitor-segment msc_i. Let $\Gamma^{-1}(c_i) = \{msc_j | (msc_j, c_i) \in E'\}$ denote the set of monitor-segments monitoring a connection c_i.

A connection is called $UnIdentified$ if we cannot obtain the status of the connection directly from the set of all monitor-segments' status in the network. Figure 4.5 shows an example to help understand this concept. A network and its connections are shown in Figure 4.5. If connection c_1 is the OAF, according to the truth table we can identify the status for both the monitor-segments and connections, as shown in Table 4.2. The monitor-segments can only identify the status of c_2 and c_3 as IF and the status of connection c_1 as *uncertain* according to both monitor-segments' results.

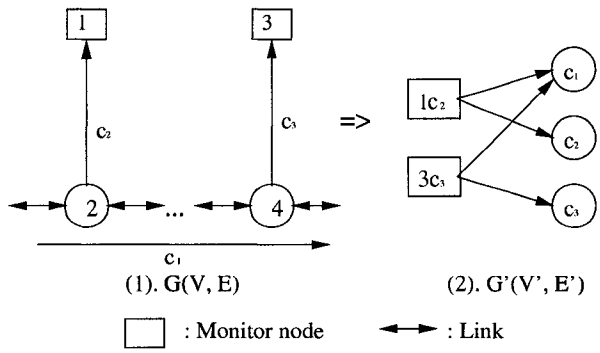


Figure 4.5 UnIdentified connection

Table 4.2 Status of the connections and the monitor-segments shown in Figure 4.5

monitor-segments	$S(msc)$	$S(c_1)$	$S(c_2)$	$S(c_3)$
$S(1c_2)$	A	*uncertain*	*uncertain*	IF
$S(3c_3)$	A	*uncertain*	IF	*uncertain*

4.1.2 One-Crosstalk-Attack-Diagnosable Conditions

In this section, we establish the exact diagnosis conditions by using a set of lemmas and theorems.

Lemma 1: In any network, if this system is one-OAF diagnosable, then,

$|UnIdentified\ connection| \leq 1$.

Proof. Obvious. □

Lemma 2: For an arbitrary connection c_i, if c_i is UnIdentified, then $S(msc_i) = A$ for $\forall\ msc_i \in \Gamma^{-1}(c_i)$.

Proof. Suppose one $msc_k \in \Gamma^{-1}(c_i)$ has $S(msc_k) = \bar{A}$. Then, according to Table 4.1, $S(c_i) = IF$, and this contradicts the condition of the statement of Lemma. □

Theorem 1 (Necessary and Sufficient Condition for One-Crosstalk Attack):

In a network with at most one OAF existing at a time, $\forall c_i, c_j \in C$, $c_i \neq c_j$, if

$$\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j),$$

then for this network with the connection set C, $|UnIdentified\ connection| \leq 1$ holds.

What this theorem states is that for any arbitrary pair of connections c_i and c_j in a given monitor-segment graph G', if the set of monitor-segment of connection c_i is not the same as the set of monitor-segment of connection c_j, then there is no more than one UnIdentified connection for this network with the connection set C.

Proof. Necessity:

Suppose $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$, then there are two possibilities.

(1) $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) = \emptyset$. Then for all $msc_x \in MSC$, there always exists a $non - monitoring$ relation to both c_i and c_j. If for all $msc_x \in MSC$, $S(msc_x) = \bar{A}$, then according to Table 4.1, the status for both c_i and c_j will be uncertain. All other connections will have a status of IF. Thus, these two connections will be UnIdentified, and $|UnIdentified\ connection| > 1$.

(2) $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) \neq \emptyset$. Figure 4.6(1) shows a network which has 3 nodes and two connections, c_i and c_j. The only way to make $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) \neq \emptyset$ is to let node 1 and 3 be monitor nodes and node 2 be non-monitor node, as shown in Figure 4.6(2). Figure 4.6(3) shows the monitor-segment graph G'. Suppose c_i is the OAF. Then both monitor-segments would have state A, which makes both c_i and c_j in uncertain status. Again, $|UnIdentified\ connection| > 1$.

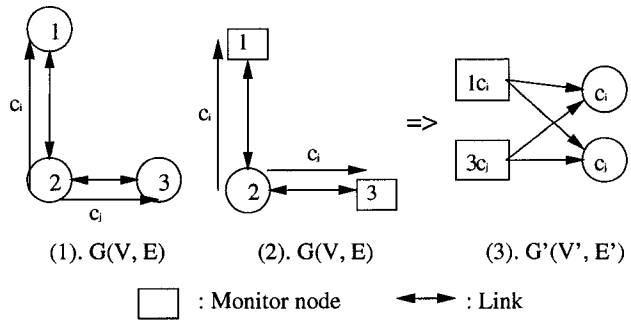


Figure 4.6 Two connections with the same $\Gamma^{-1}(c)$ sets

Sufficiency:

Suppose $|UnIdentified\ connection| > 1$. Then, there are only three possibilities:

(1) at least 2 UnIdentified connections have $\Gamma^{-1}(c) = \emptyset$. Arbitrarily pick a pair of connections c_i and c_j from this UnIdentified connection set, and we get $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j) = \emptyset$. Obviously, this contradicts our original statement of the theorem.

(2) one UnIdentified connection c_i has $\Gamma^{-1}(c_i) = \emptyset$, and at least another UnIdentified connection c_j has $\Gamma^{-1}(c_j) \neq \emptyset$. Then, according to Lemma 2, in graph G', there exists

at least one edge (msc_j, c_j) while $S(msc_j) = A$. Because of $\Gamma^{-1}(c_i) = \emptyset$, the monitor-segment msc_j has non-monitoring on c_i. According to Table 4.1, if $S(msc_j) = A$, then $S(c_i) = IF$. Thus, c_i is not UnIdentified. This contradicts the assumption.

(3) at least 2 UnIdentified connections have $\Gamma^{-1}(c) \neq \emptyset$. Arbitrarily select two connections c_i and c_j from this set. There are two possible cases:

Case I: $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. Suppose one monitor-segment $msc_i \in \Gamma^{-1}(c_i)$ but $msc_i \notin \Gamma^{-1}(c_j)$. Then, edge (msc_i, c_j) does not exist in graph G'. Thus, monitor-segment msc_i must have non-monitoring on c_j. Because c_i is UnIdentified, according to lemma 2, $S(msc_i) = A$, which implies that $S(c_j) = IF$, referring to Table 4.1. Thus c_j is not UnIdentified, which contradicts our assumption.

Case II: $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$. This contradicts the condition.

Thus, if $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, then $|UnIdentified\ connection| \leq 1$ always holds. □

4.1.3 Global Status of a Connection According to Monitor-Segment with One-OAF Condition

For a given monitor-segment msc_i, there are only two relations between msc_i and an arbitrary connection c_j: monitoring or non-monitoring. Let monitoring and non-monitoring relations be denoted by two values: 1 and 0, respectively. Then, a vector $\overrightarrow{r_i}$ can be used to denote such relation between msc_i and all connections in the network:

$\overrightarrow{r_i} = \{r_i(c_j) | c_j \in C\}$,

and a *Relation Matrix* $\mathbb{R}$ can be created as follows.

$$\mathbb{R} = \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \cdots \\ \overrightarrow{r_m} \end{pmatrix} = \begin{pmatrix} r_1(c_1) & r_1(c_2) & \cdots & r_1(c_n) \\ r_2(c_1) & r_2(c_2) & \cdots & r_2(c_n) \\ \cdots & \cdots & \cdots & \cdots \\ r_m(c_1) & r_m(c_2) & \cdots & r_m(c_n) \end{pmatrix};$$

where $r_i(c_j)$ denotes the relation between msc_i and c_j, i.e.,

$$r_i(c_j) = \begin{cases} 1, & if\ msc_i\ monitor\ c_j \\ 0, & if\ msc_i\ not\ monitor\ c_j \end{cases}.$$

With a given status of the monitor-segment, we can get the corresponding status of all connections. For example, in Table 4.2, according to the status of monitor-segment $S(1c_2)$, the status of all three connections, $S(c_1)$, $S(c_2)$, and $S(c_3)$, can be derived. Monitor-segment $1c_2$ monitors c_1 and c_2, but does not monitor c_3. Because $S(1c_2)$ is A, according to Table 4.1, the status of c_1 should be $S(c_1) = uncertain$, the status of c_2 should be $S(c_2) = uncertain$, and the status of c_3 should be $S(c_3) = IF$. Let us assume that there are a total of n connections and m monitor-segments in the network. Let vector $\overrightarrow{S_i(c)} = \{S_i(c_1), S_i(c_2), \ldots, S_i(c_n)\}$ denote all connections' status given by msc_i, where $S_i(c_j)$ denotes status of c_j derived from status of msc_i.

Now, set two possible connection status, IF and $uncertain$, as 1 and 0, respectively. Similarly, set two possible monitor-segment status, A and $\bar{A}$, as 1 and 0, respectively. Then, according to the truth table, Table 4.1, we can derive $S_i(c_j)$ from $S(msc_i)$ and $r_i(c_j)$:

$$S_i(c_j) = S(msc_i) \oplus r_i(c_j);$$

while $\overrightarrow{S_i(c)}$ from $S(msc_i)$ and $\overrightarrow{r_i}$:

$$\overrightarrow{S_i(c)} = [S(msc_i) \cdot \vec{1}] \oplus \overrightarrow{r_i};$$

where $\vec{1}$ is a $1 \times n$ vector, and $\oplus$ is XOR.

Then, a *Status Matrix* can be obtained as follows.

$$\begin{pmatrix} \overrightarrow{S_1(c)} \\ \overrightarrow{S_2(c)} \\ \cdots \\ \overrightarrow{S_m(c)} \end{pmatrix} = \begin{pmatrix} S_1(c_1) & S_1(c_2) & \cdots & S_1(c_n) \\ S_2(c_1) & S_2(c_2) & \cdots & S_2(c_n) \\ \cdots & \cdots & \cdots & \cdots \\ S_m(c_1) & S_m(c_2) & \cdots & S_m(c_n) \end{pmatrix}$$

$$= \{ \begin{pmatrix} S(msc_1) \\ S(msc_2) \\ \cdots \\ S(msc_m) \end{pmatrix} \times \overrightarrow{1} \} \oplus \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \cdots \\ \overrightarrow{r_m} \end{pmatrix}.$$

Let $S(c_j)$ denote the logical OR of jth column in the above matrix, and let $\bigvee$ denote the logical OR operation:

$$S(c_j) = \bigvee_{i=1}^{m} S_i(c_j) = \bigvee_{i=1}^{m} [S(msc_i) \oplus r_i(c_j)].$$

Now, if we define a new operation $*$ as:

$$\overrightarrow{X} * \overrightarrow{Y}^T = \bigvee_{i=1}^{n} [x_i \oplus y_i]$$

where $\overrightarrow{X}$ and $\overrightarrow{Y}$ are $1 \times n$ vectors and x_i and y_i are their elements,

then vector $\overrightarrow{S(c)}$ can be denoted by $S(msc_i)$ and its relation matrix as following:

$$\overrightarrow{S(c)} = \begin{pmatrix} S(c_1) & \cdots & S(c_n) \end{pmatrix}$$

$$= \begin{pmatrix} S(msc_1) & \cdots & S(msc_m) \end{pmatrix} * \begin{pmatrix} r_1(c_1) & \cdots & r_1(c_n) \\ \cdots & \cdots & \cdots \\ r_m(c_1) & \cdots & r_m(c_n) \end{pmatrix}.$$

The global status of connection c_j can be obtained as

$$Status\ of\ c_j = \begin{cases} IF, & if\ S(c_j) = 1 \\ UnIdentified, & if\ S(c_j) = 0 \end{cases}.$$

For example, as shown in Figure 4.5, if connection c_1 is the OAF, then, $S(1c_2) = A = 1$, $S(3c_3) = A = 1$. According to Figure 4.5(2), we can get the relation between $1c_2$ and other connections as

$\overrightarrow{r_{1c_2}} = \{r_{1c_2}(c_1), r_{1c_2}(c_2), r_{1c_2}(c_3)\} = \{1, 1, 0\}$,

and the relation between $3c_3$ and other connections as

$\overrightarrow{r_{3c_3}} = \{r_{3c_3}(c_1), r_{3c_3}(c_2), r_{3c_3}(c_3)\} = \{1, 0, 1\}$.

Then,

$$\begin{aligned}
\overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) \end{pmatrix} \\
&= \begin{pmatrix} S(1c_2) & S(3c_3) \end{pmatrix} * \begin{pmatrix} r_{1c_2}(c_1) & r_{1c_2}(c_2) & r_{1c_2}(c_3) \\ r_{3c_3}(c_1) & r_{3c_3}(c_2) & r_{3c_3}(c_3) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}.
\end{aligned}$$

Because $S(c_1) = 0$, connection c_1 must be the OAF in the network.

4.1.4 Computational Complexity

This method can be easily applied to any large or small size network. Let $D(u)$ denote degree of node u. Suppose we have $|M|$ monitors in the network, and $Max\{D(m)\} = d_M, m \in M$, then the total number of monitor-segment will be no more than $|M| \times d_M$. Also, if we assume that there are no more than $|C|$ connections in the whole network, then the relation matrix size will be no more than $(|M| \times d_M) \times |C|$. Thus, for determining one OAF, the computation complexity will be $O((|M| \times d_M)^2 \times |C|)$, and the only operations needed in the computation are $+$ and $\oplus$.

4.2 Necessary and Sufficient Condition for k Crosstalk Attack in the Network

In the previous section, we provided a necessary and sufficient condition for one-OAF diagnosable network. However, in most cases, attackers tend to introduce more than one attack signal into the network simultaneously. Thus, the capability to localize more than one co-existing attack signal in an AON is more important in practical respects. We extend the one-OAF-diagnosable condition into k-OAF-diagnosable network [44].

4.2.1 Monitor-Segment

We use the same concept of monitor-segment here as in the one-OAF-diagnosable network. However, the truth table in Table 4.1 will change. In a one-OAF diagnosable network, if status of one msc is A, then all connections not monitored by this msc can be automatically set to $\bar{A}$. However, if there are more than one OAF in the network simultaneously, this conclusion is not true. Those connections not monitored by this msc can still be either OAF or IF. Table 4.3 shows the relations between a monitor-segment status and its monitoring connection's status.

Table 4.3 Truth Table for monitor-segment and its monitoring/non-monitoring connections with more than one OAF in the network

Relation	$S(msc)$	$S(c)$
msc monitoring c	A	*uncertain*
(msc, c)	$\bar{A}$	IF
msc non-monitoring c	A	*uncertain*
	$\bar{A}$	*uncertain*

The big difference between Table 4.1 and Table 4.3 is that in Table 4.1, an A status

monitor-segment implies that all its non-monitoring connections' status are IF, while in Table 4.3, an A status monitor-segment cannot imply that any of its non-monitoring connections' status is IF.

Similarly, a connection is called $UnIdentified$ if we cannot obtain the status of the connection directly from the set of all monitor-segments' status in the network. A network and its connections are shown in Figure 4.5. If connection c_2 is the OAF, then according to the truth table we can identify the status for both the monitor-segments and connections, as shown in Table 4.4. The monitor-segments can only identify the status of c_3 as IF, and status of connections c_1 and c_2 as *uncertain* according to both monitor-segments' results.

Table 4.4 Status of the connections and the monitor-segments shown in Figure 4.5

monitor-segments	$S(msc)$	$S(c_1)$	$S(c_2)$	$S(c_3)$
$S(1c_2)$	A	*uncertain*	*uncertain*	*uncertain*
$S(3c_3)$	$\bar{A}$	*uncertain*	*uncertain*	IF

4.2.2 k-Crosstalk-Attack-Diagnosable Condition

In this section, we establish the diagnosis conditions for k-crosstalk attacks by using a set of lemmas, theorems, and corollaries.

Lemma 3: If $msc \notin \Gamma^{-1}(c)$, c cannot affect the msc status even if c is an OAF.

Proof. According to truth Table 4.3, no matter whether a connection c is in *Uncertain* status or in IF status, if a $msc \notin \Gamma^{-1}(c)$, then the status of this monitor segment msc is always unknown.

□

Lemma 4: For a connection $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, $c_i \in C$ and $\{c_{j_1}, ..., c_{j_k}\} \subseteq C$, if $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, then $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_m}^{j_n} \Gamma^{-1}(c_j)$, where $\{c_{j_m}, ..., c_{j_n}\} \subseteq \{c_{j_1}, ..., c_{j_k}\}$.

Proof. Since $\{c_{j_m}, ..., c_{j_n}\} \subseteq \{c_{j_1}, ..., c_{j_k}\}$, $\bigcup_{j=j_m}^{j_n} \Gamma^{-1}(c_j) \subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is always true. Moreover, since $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_m}^{j_n} \Gamma^{-1}(c_j)$ is also always true. □

Lemma 5: If a connection c is an OAF, then c must be in $UnIdentified$ status.

Proof. If c is an OAF, all $msc \in \Gamma^{-1}(c)$ are in A status, thus all $msc \in \Gamma^{-1}(c)$ indicate that c's status is uncertain. According to definition, c is in $UnIdentified$ status. □

Corollary 1: If there is a total of m $UnIdentified$ connections in the network, then there are no more than m OAFs in the network simultaneously.

Proof. If there are more than m OAFs in the network simultaneously, then according to Lemma 5, all these OAFs must be in $UnIdentified$ status, which contradicts our assumption. Thus, if there are total m $UnIdentified$ connections in the network, then there are no more than m OAFs in the network simultaneously. □

Theorem 2: For any connection $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, where $c_i \in C$, and $\{c_{j_1}, ..., c_{j_k}\} \subseteq C$ is an arbitrary subset of existing connections in the network, if $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, and there are $k+1$ $UnIdentified$ connections in the network, then there must be at least $k+1$ OAFs in the network.

Proof. We prove this theorem by induction.

Initial step: suppose $k = 1$. Then, $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j)$, for $\forall c_i, c_j \in C$. Assume an arbitrary pair of connections c_a and c_b are $UnIdentified$ connections, but there is no more than one OAF in the network. There can be 3 possibilities.

1. There is no OAF in the network. Then, every *msc* in the network should be in $\bar{A}$ status, thus, all connections should be in IF status. This contradicts our assumption.

2. One of c_a or c_b is an OAF. Without loss of generality, assume c_b is an OAF. Since $\Gamma^{-1}(c_a) \not\subseteq \Gamma^{-1}(c_b)$, there exists at least one *msc* m such that $m \in \Gamma^{-1}(c_a)$ and $m \notin \Gamma^{-1}(c_b)$. According to Lemma 3, c_b cannot affect the status of m. Then, m must be in $\bar{A}$ status, which implies c_a is not an $UnIdentified$ connection. This again contradicts our assumption.

3. Another OAF c_m exists. According to the given condition, $\Gamma^{-1}(c_a) \not\subseteq \Gamma^{-1}(c_m)$. Thus there exists at least one *msc* m such that $m \in \Gamma^{-1}(c_a)$ and $m \notin \Gamma^{-1}(c_m)$ must exist. According to Lemma 3, c_m cannot affect the status of m. Then, m must be in $\bar{A}$ status, which implies c_a is not $UnIdentified$ connection. This again contradicts our assumption.

   Thus, the number of OAFs, $|OAF|$, is at least 2, which implies that this theorem is true when $k = 1$.

Induction step: suppose this theorem is true for $k-1$ (i.e., $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_{k-1}} \Gamma^{-1}(c_j)$, where $c_i \notin \{c_{j_1}, ..., c_{j_{k-1}}\}$, $c_i \in C$, and $\{c_{j_1}, ..., c_{j_{k-1}}\} \subseteq C$ is an arbitrary subset of existing connections in the network), then there must be at least k OAFs in the network simultaneously if there exist k $UnIdentified$ connections in the network.

Suppose $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is true for all $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, and suppose $k+1$ $UnIdentified$ connections in the network are c_{n_1}, ..., $c_{n_{k+1}}$. Since $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$, from Lemma 4, $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_{k-1}} \Gamma^{-1}(c_j)$ is also satisfied. Since there are at least k $UnIdentified$ connections in the network, therefore there are at least k OAFs, c_{m_1}, ..., c_{m_k}, exist. According to our assumption, $\Gamma^{-1}(c_{n_i}) \not\subseteq \bigcup_{m=m_1}^{m_k} \Gamma^{-1}(c_m)$, there exists a *msc* msc_{n_i} such that $msc_{n_i} \in \Gamma^{-1}(c_{n_i})$ and $msc_{n_i} \notin \bigcup_{m=m_1}^{m_k} \Gamma^{-1}(c_m)$.

According to Lemma 3, all $c_m \in \{c_{m_1}, ..., c_{m_k}\}$ cannot affect msc_{n_i}. Thus there must exist at least one extra OAF that affects the status of msc_{n_i}. Therefore, at least $k+1$ OAFs must exist in the network. Thus the theorem holds for all values of k. □

Theorem 3 (Necessary and Sufficient Condition for k-Crosstalk Attacks) :

In a network containing up to k OAFs simultaneously, $\forall c_i$, c_{j_1}, ..., $c_{j_k} \in C$, $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, if

$$\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$$

then for this network with the connection set C, $|UnIdentified\ Connection| \leq k$ holds.

What this theorem states is that for one connection c_i and an arbitrary set of k connections $\{c_{j_1}, ..., c_{j_k}\}$, where c_i is not in $\{c_{j_1}, ..., c_{j_k}\}$, if the set of monitor-segment of connection c_i is not a subset of the union of monitor-segment set for connections $\{c_{j_1}, ..., c_{j_k}\}$, then there is no more than k UnIdentified connection for this network if there are at most k OAFs existing simultaneously in the network.

Proof. Necessity:

Without loss of generality, suppose in a subset of k connections (i.e., $\{c_{j_1}, ..., c_{j_k}\}$) all are OAFs. According to lemma 5, all OAFs are unidentified. Then, for some connection $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, there are two possibilities.

1. $\Gamma^{-1}(c_i) = \emptyset$. Obviously, $\Gamma^{-1}(c_i) \subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$. Since there is no $msc \in \Gamma^{-1}(c_i)$, c_i is unidentified. According to lemma 5, all OAFs are unidentified along with $\{c_{j_1}, ..., c_{j_k}\}$, and thus $|UnIdentified\ Connection| > k$, this contradicts our assumption.

2. $\Gamma^{-1}(c_i) \neq \emptyset$ and suppose $\Gamma^{-1}(c_i) \subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$. Then, for all $msc \in \Gamma^{-1}(c_i)$, $msc \in \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ holds.

Obviously, all $msc \in \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ must be in A status. Therefore, $msc \in \Gamma^{-1}(c_i)$ are also in A state, thus c_i is also UnIdentified and $|UnIdentified\ Connection| > k$. This contradicts our assumption again.

Sufficiency:

Suppose $|UnIdentified\ Connection| \geq k+1$, and for every unidentified connection c, $\Gamma^{-1}(c) \neq \emptyset$. Assume that for any connection c_i and any arbitrary subset of k connections $\{c_{j_1}, ..., c_{j_k}\}$, $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$, $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is always satisfied. According to Theorem 2, at this time, the number of OAFs is at least $k+1$, which contradicts our assumption that there are no more than k OAFs in the network simultaneously.

Thus, the theorem holds.

□

Corollary 2: For any connection $c_i \notin \{c_{j_1}, ..., c_{j_k}\}$ where $c_i \in C$ and any arbitrary subset $\{c_{j_1}, ..., c_{j_k}\} \subseteq C$ in the network, if $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_k} \Gamma^{-1}(c_j)$ is always true, then for $m \leq k$,

1. there are no more than m *UnIdentified* connections in the network if there are only m OAFs in the network;
2. there are exactly m OAFs if there exist m *UnIdentified* connections;
3. if there exist m *UnIdentified* connections, these m connections must be m OAFs.

Proof. 1. According to the condition, if c_i is not an OAF, then $\Gamma^{-1}(c_i) \not\subseteq \bigcup_{j=j_1}^{j_m} \Gamma^{-1}(c_j)$, where c_j is one of m OAF connections, is always true. Thus, there exists a $msc_i \in \Gamma^{-1}(c_i)$ but $msc_i \notin \bigcup_{j=j_1}^{j_m} \Gamma^{-1}(c_j)$. According to Lemma 3, none of these OAFs can affect the state of msc_i. Thus, no connections except OAFs will be in *UnIdentified* status.

2. According to Corollary 1, $|OAF| \leq m$, while according to Theorem 2, $|OAF| \geq m$, thus $|OAF| = m$.

3. According to result 2, if there are $m \leq k$ *UnIdentified* connections, there must be exactly m OAFs; while according to result 1, if there are $m \leq k$ OAFs, then no more than m connections will be *UnIdentified* connections. According to Lemma 5, all OAFs must be *UnIdentified* connections. Therefore, all these m OAFs should be in *UnIdentified* status. Thus, if there are $m \leq k$ *UnIdentified* connections in the network, these m connections must be the OAFs.

□

4.2.3 Global Status of a Connection According to Monitor-Segment

As with one-OAF diagnosable networks, we can use matrices and their operations to denote the relation between the status of *msc* and connections.

Again, let the two possible relations between a given monitor-segment msc_i and an arbitrary connection c_j: monitoring or non-monitoring, be denoted by 1 and 0, respectively. Then, a vector $\overrightarrow{r_i}$ can be used to denote such relation between msc_i and all connections in the network:

$\overrightarrow{r_i} = \{r_i(c_j) | c_j \in C\}$,

and a *Relation Matrix* $\mathbb{R}$ can be created as:

$$\mathbb{R} = \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \cdots \\ \overrightarrow{r_m} \end{pmatrix} = \begin{pmatrix} r_1(c_1) & r_1(c_2) & \cdots & r_1(c_n) \\ r_2(c_1) & r_2(c_2) & \cdots & r_2(c_n) \\ \cdots & \cdots & \cdots & \cdots \\ r_m(c_1) & r_m(c_2) & \cdots & r_m(c_n) \end{pmatrix};$$

where n denotes total number of connections, m denotes total number of monitor-

segments in the network, and $r_i(c_j)$ denotes the relation between msc_i and c_j:

$$r_i(c_j) = \begin{cases} 1, & if\ msc_i\ monitor\ c_j \\ 0, & if\ msc_i\ not\ monitor\ c_j \end{cases}.$$

With a given status of the monitor-segment, we can get the corresponding status of all connections. For example, in Table 4.4, according to the status of monitor-segment $S(3c_3)$, the status of connection c_3, $S(c_3)$, can be derived. Let vector $\overrightarrow{S_i(c)} = \{S_i(c_1), S_i(c_2), \ldots, S_i(c_n)\}$ denote all connections' status given by msc_i, where $S_i(c_j)$ denotes status of c_j derived from status of msc_i.

Now, set two possible connection status, IF and *uncertain*, as 1 and 0, respectively. Similarly, set two possible monitor-segment status, A and $\bar{A}$, as 1 and 0, respectively. Then, according to truth table Table 4.3, we can derive $S_i(c_j)$ from $S(msc_i)$ and $r_i(c_j)$:

$$S_i(c_j) = \{S(msc_i) \times r_i(c_j)\} \oplus r_i(c_j),$$

while $\overrightarrow{S_i(c)}$ from $S(msc_i)$ and $\overrightarrow{r_i}$ is

$$\overrightarrow{S_i(c)} = \{[S(msc_i) \cdot \vec{1}] \times \overrightarrow{r_i}\} \oplus \overrightarrow{r_i},$$

where $\vec{1}$ is a $1 \times n$ vector, $\times$ is AND, and $\oplus$ is XOR.

Then, a *Status Matrix* can be obtained.

$$\begin{pmatrix} \overrightarrow{S_1(c)} \\ \overrightarrow{S_2(c)} \\ \cdots \\ \overrightarrow{S_m(c)} \end{pmatrix} = \begin{pmatrix} S_1(c_1) & S_1(c_2) & \ldots & S_1(c_n) \\ S_2(c_1) & S_2(c_2) & \ldots & S_2(c_n) \\ \cdots & \cdots & \cdots & \cdots \\ S_m(c_1) & S_m(c_2) & \ldots & S_m(c_n) \end{pmatrix}$$

$$= \{[\begin{pmatrix} S(msc_1) \\ S(msc_2) \\ \cdots \\ S(msc_m) \end{pmatrix} \cdot \vec{1}] \times \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \cdots \\ \overrightarrow{r_m} \end{pmatrix}\} \oplus \begin{pmatrix} \overrightarrow{r_1} \\ \overrightarrow{r_2} \\ \cdots \\ \overrightarrow{r_m} \end{pmatrix}.$$

Let $S(c_j)$ denote the logical OR of jth column in above matrix, and let $\bigvee$ denote the logical OR operation:

$$S(c_j) = \bigvee_{i=1}^{m} S_i(c_j) = \bigvee_{i=1}^{m} \{[S(msc_i) \times r_i(c_j)] \oplus r_i(c_j)\}.$$

Now, if we define a new operation $*$ as

$$\overrightarrow{X} * \overrightarrow{Y}^T = \bigvee_{i=1}^{n} \{[x_i \times y_i] \oplus y_i\}$$

where $\overrightarrow{X}$ and $\overrightarrow{Y}$ are $1 \times n$ vectors and x_i and y_i are their elements;

then, vector $\overrightarrow{S(c)}$ can be denoted by $S(msc_i)$ and its relation matrix as follows:

$$\begin{aligned} \overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & \dots & S(c_n) \end{pmatrix} \\ &= \begin{pmatrix} S(msc_1) & \dots & S(msc_m) \end{pmatrix} * \begin{pmatrix} r_1(c_1) & \dots & r_1(c_n) \\ \dots & \dots & \dots \\ r_m(c_1) & \dots & r_m(c_n) \end{pmatrix}. \end{aligned}$$

The global status of connection c_j can be obtained as:

$$Status\ of\ c_j = \begin{cases} IF, & if\ S(c_j) = 1 \\ UnIdentified, & if\ S(c_j) = 0 \end{cases}.$$

According to Corollary 2, if the status of connection c_j is $UnIdentified$, then c_j must be an OAF. This provides the algorithm for locating the attack connections of each wavelength.

For example, as shown in Figure 4.7, there are two crosstalk attack connections, c_1 and c_2, and c_3 is non-attack connection. There are three monitor-segments: $1c_1$, $1c_2$, and $1c_3$. According to monitor-segment definition, $\Gamma^{-1}(c_1) = \{1c_1\}$, $\Gamma^{-1}(c_2) = \{1c_2\}$, and $\Gamma^{-1}(c_3) = \{1c_3\}$. This satisfies the k-crosstalk-diagnosable condition. Thus, we can determine which connections are attack connections according to these monitor-

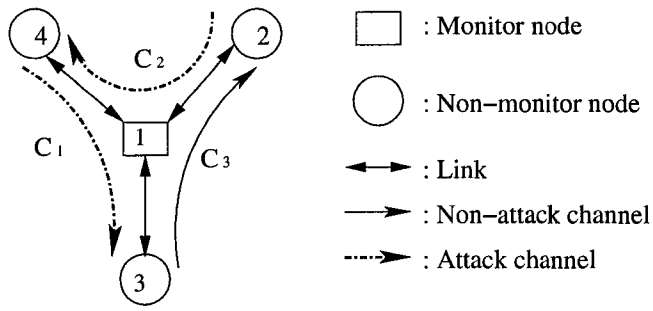


Figure 4.7 Two attacks in AON

segments' status. In this example, relation matrix $\mathbb{R}$ is:

$$\mathbb{R} = \begin{pmatrix} r_{1c_1}(c_1) & r_{1c_1}(c_2) & r_{1c_1}(c_3) \\ r_{1c_2}(c_1) & r_{1c_2}(c_2) & r_{1c_2}(c_3) \\ r_{1c_3}(c_1) & r_{1c_3}(c_2) & r_{1c_3}(c_3) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and the status of all monitor-segments is:

$$\overrightarrow{S(msc)} = \begin{pmatrix} S(1c_1) & S(1c_2) & S(1c_3) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}.$$

Thus,

$$\begin{aligned}
\overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) \end{pmatrix} \\
&= \begin{pmatrix} S(1c_1) & S(1c_2) & S(1c_3) \end{pmatrix} * \begin{pmatrix} r_{1c_1}(c_1) & r_{1c_1}(c_2) & r_{1c_1}(c_3) \\ r_{1c_2}(c_1) & r_{1c_2}(c_2) & r_{1c_2}(c_3) \\ r_{1c_3}(c_1) & r_{1c_3}(c_2) & r_{1c_3}(c_3) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}.
\end{aligned}$$

Because $S(c_1) = 0$, $S(c_2) = 0$, and $S(c_3) = 1$, connections c_1 and c_2 must be the OAFs in this network.

4.2.4 Computational Complexity

Suppose we have $|M|$ monitors in the network, and $Max\{D(m)\} = d_M, m \in M$, then the total number of monitor-segment will be no more than $|M| \times d_M$. Also, if we assume that there are no more than $|C|$ connections in the whole network, then the relation matrix size will be no more than $(|M| \times d_M) \times |C|$. The computational complexity of first part, $[S(msc_i)] \times \mathbb{R}$, is $O((|M| \times d_M)^2 \times |C|)$, while the computational complexity of second part, two $(|M| \times d_M) \times |C|$ size matrices $\oplus$, is $O(|M| \times d_M \times |C|)$. Thus, for determining k OAFs, the computation complexity will be $O((|M| \times d_M + 1) \times |M| \times d_M \times |C|) = O((|M| \times d_M)^2 \times |C|)$, and the only operations needed in the computation are $+$ and $\oplus$. Thus this method is scalable and can be easily applied to a large network.

CHAPTER 5 SPARSE MONITORING POLICIES AND ROUTING ALGORITHMS

In previous chapters, we analyzed the AON node model, crosstalk attack model, and monitor model. Moreover, we proposed the monitor-segment concept. Based on this concept, we developed and proved the necessary and sufficient condition for identifying one malicious attack source on each wavelength in an AON. After that, we extended this result to a more general case and proved the necessary and sufficient condition for identifying more than one coexisting crosstalk attack source on each wavelength in an AON. Now, based on these conditions, we develop some practical sparse monitor algorithms to identify every crosstalk attack in an AON.

5.1 Introduction of Monitor Placement Policies and Routing Policies

According to previous analysis, to find out the exact location of the OAF in a network, we have to determine a monitor placement and a routing policy that work together in such a way that we can meet the necessary and sufficient condition. We cannot satisfy this condition if we ignore either of them. For example, according to Theorem 1, all connections except one should be monitored by at least one monitor-segment. Thus, if several connections neither traverse a monitor nor pass through those nodes next to a monitor, then none of these connections can be monitored by any monitor-segment, and we cannot determine the attack status of the network. Thus, we can understand the

reason why both monitor placement and routing policy are so important in the crosstalk attack detection and localization problem.

Monitor nodes are used to provide monitor-segments for existing connections. Because the cost of monitors will be expensive in the near future, network designer cannot anticipate to put monitors on every node. Therefore, we propose a monitor placement policy to place monitors on some critical nodes only. For monitor placement policies, we anticipate providing answers to questions such as: Does sparse monitors provide sufficient diagnostic information for attack management system? How many monitors are required for diagnostic purpose? Is there any upper-bound or lower-bound for that? What is the relation between a monitor placement policy and its corresponding routing policy? How can a monitor placement policy affect the routing policy?

In this chapter, several sparse monitoring policies are propsed. We prove that these policies satisfy our sufficiency conditions. According to the necessary and sufficient conditions, there is no special requirement for the number of monitors. The only lower bound is that there must be at least one monitor in the network so that monitor-segment required by diagnosis can be provided. The routing policy is totally interwoven with the monitor placement policy. With a given monitor placement policy, routing policy need to route connections to traverse some monitors or some nodes close to monitors to meet the requirements. Obviously, the fewer is the number of monitors in a network, the more restriction will be there for routing policies, and correspondingly, the higher blocking probability for connections. Monitor placement problem is studied in [40, 41, 42, 43, 44]. Because how to place sparse monitors in a given network is a difficult problem, only heuristic solutions are given in this chapter.

Routing policies are always interwoven with monitor placement policies. In the area of routing policies, we want to solve the following problems: How should routes be assigned to connections in anticipation of crosstalk attacks? Does route assignment in anticipation of a coordinated attack use more resources?

According to the necessary and sufficient conditions, when a monitor placement policy is determined, the corresponding routing policy should guarantee that all connections should obtain a different monitor-segment set from other connection or connections. With this restriction, routing policies tend to use more resources to satisfy the necessary and sufficient conditions for diagnosis, and this always leads to higher traffic blocking probability. This is the tradeoff between monitor placement policies and corresponding routing policies.

As in Chapter 4, we first propose algorithms for the special case, which is that only one OAF exists on any wavelength in an AON, and prove it to be sufficient to localize the OAF in an AON. Then we discuss the general case.

5.2 Sparse Monitoring Policies for Single OAF

First, we assume that only one OAF exists in an AON. Sparse monitoring solution with one-OAF condition has been studied in this chapter and are also presented in [41, 42, 43]. Before describing the algorithm, we need the following definitions.

1. *One-hop-distance monitor (***OHM***):* If a monitor is connected directly to a non-monitor node u, then this monitor is an OHM to this non-monitor node. $OHM(u)$ denotes the set of OHM for node u.

2. *Degree of a node:* The degree of a node u is the number of links that intersect with this node, denoted by $D(u)$.

3. *Pendant node:* A node with degree one is called a pendant node.

5.2.1 Sparse Monitoring Policy I

To satisfy the necessary and sufficient condition proved in Theorem 1, we have to develop not only monitor placement policies, but also routing policies as well as test con-

nection setup policies. The following section describes the policies required to guarantee a network to be an one-OAF diagnosable network.

5.2.1.1 Description of Policy I

1. **Monitor placement policy**

   To guarantee the exact location of the OAF in a network, we suggest the following sparse monitor placement policy.

   (a) for non-monitor node u, $D(u) \geq 2$;

   (b) a non-monitor node u must have $D(u)$ OHMs;

   (c) a node u with a pendant node as its neighbor must be a monitor node.

2. **Test connection setup policy**

   We assume that each link in the network is bi-directional so that there is a fiber for each of two directions in each link. According to our monitoring mechanism, there are two kinds of connections: one is the *normal connection* which is set up by users, and the other is the *test connection* which is requested by the network management system. A test connection is an important method in determining if a node is a PAN or not. We use the following rule to set up test connections:

   for a non-monitor node, if there is a normal connection on wavelength λ terminating at this node and no normal connection provides a monitor-segment on the corresponding link, then one test connection from this node to each OHM is needed.

3. **Routing policy**

   To guarantee the exact location of the OAF in a network, we use the following rules to set up a connection:

(a) for any two of the normal connections (excluding test connection) originating from a same non-monitor node, at least one must pass through three different nodes, including source and destination;

(If $\forall c_i, c_j \in R$, and $c_i = \{u_0, \dots\}$, $c_j = \{u_0, \dots\}$, then always $\exists\{u_a, u_b, u_c\} \subset c_i$ but $\not\subset c_j$ or $\exists\{u_a, u_b, u_c\} \subset c_j$ but $\not\subset c_i$.)

(b) normally we use the shortest path algorithm except for the above case.

According to our crosstalk attack model, the crosstalk attack only affects the same wavelength connection at the wavelength selective switch. To simplify our analysis, in the following parts we always assume that there is no wavelength converter in the whole network, and for each link only one fiber exists in each direction.

In the following, based on previous models and policies, we prove that a network is always one-OAF diagnosable.

Claim 1: With above monitor placement, test connection setup, and routing policies, a network with one fiber on each link and without a wavelength converter is one-OAF diagnosable on each wavelength.

Proof. With a given network denoted by graph $G(V, E)$, let M denote the set of monitor nodes, and let N denote the set of non-monitor nodes, $M \subseteq V$, $N \subset V$, and $M \bigcup N = V$. Let $C = R \bigcup T$ denote the set of connections in the network, where R is the regular set of connections, and T is the set of test connections. Let c_i be a connection consisting of nodes $\{u_0, u_1, u_2, \dots, u_k, \dots\}$. Let $U(c_i)$ denote the set of nodes on connection c_i's path. Then, c_{ij} denotes an one-hop segment $(u_j \rightarrow u_{j+1})$ on connection c_i.

First, in each link, we assume there is only one wavelength in each direction.

1. According to the sparse monitor placement policy, for a non-monitor node each neighbor node must be a monitor node, which means on each link at least one node is a monitor node. Thus, for one connection c, at least one monitor node

$m \in U(c)$. According to the definition of monitor-segment, at least one monitor-segment monitors this connection, i.e., $\Gamma^{-1}(c) \neq \emptyset$ holds $\forall\ c \in C$.

2. According to Theorem 1, for any arbitrary pair of connections, the necessary and sufficient condition for a one-OAF diagnosable network is that the pair members' monitoring monitor-segments sets should not be the same. Now, suppose there exist two connections c_i and c_j such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$. There can be two possibilities.

   (a) At least one of them originates from a monitor node. Without loss of generality, we assume that c_i originates from monitor m. According to our earlier discussion about special cases of monitor-segment, any connection originating from a monitor can make up a special monitor-segment that would only monitor this connection. Thus, a monitor-segment mc_i made up by c_i and m does not monitor other connections including c_j, i.e., $mc_i \in \Gamma^{-1}(c_i)$, and $mc_i \notin \Gamma^{-1}(c_i)$. Then, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, which contradicts the above assumption.

   (b) None of these connections originates from a monitor node. Then, there are two possible cases.

      i. The sources of these two connections are different, i.e., c_i's source is node n_i, and c_j's source is node n_j. Suppose $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$. Because n_i, n_j are not monitors, $\{n_i, n_j\} \subseteq (U(c_i) \cap U(c_j))$ must be true. For $U(c_j)$, $UNN(n_i, c_j)$ must be a monitor, then, monitor-segment $\{n_i \rightarrow UNN(n_i, c_j)\}$ with monitor node $UNN(n_i, c_j)$ must be in $\Gamma^{-1}(c_i)$, but not in $\Gamma^{-1}(c_j)$, thus, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. This again contradicts the above assumption.

      ii. These two connections have a same non-monitor source node n. Accord-

ing to routing policy, at least one connection should pass three nodes. Without loss of generality, let us assume that c_i has at least three different nodes on its path, and the first three nodes on its path are: n, m_i, and u_i. For each link, because only one wavelength exists in each direction and at least one monitor node exists on this link, the first two nodes on c_j's path should be n and m_j, where $m_j \neq m_i$ and $m_i \notin U(c_j)$. Now let us consider node $u_i \in U(c_i)$:

A. If u_i is a monitor node, then segment $(m_i \rightarrow u_i) \in U(c_i)$ plus monitor u_i makes a monitor-segment that does not monitor connection c_j, thus, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, which contradicts the above assumption.

B. If u_i is a non-monitor node, then according to monitor placement policy, there should be at least one other OHM for node u_i besides monitor m_i. We use m', $m' \neq m_i$ to denote one of such OHMs. According to the test connection setup policy, either normal connection segments or test connections should exist as $(u_i \rightarrow m_i)$ and $(u_i \rightarrow m')$. If $u_i \in U(c_j)$, then connection c_j should be monitored by a monitor-segment composed of segment $(u_i \rightarrow m_i)$ and monitor m_i, while connection c_i should not be monitored by the same monitor-segment; or if $u_i \notin U(c_j)$, then connection c_i should be monitored by a monitor-segment composed of segment $(u_i \rightarrow m')$ and monitor m', while connection c_j should not be monitored by the same monitor-segment. We can draw the same conclusion, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, from both cases, and this also contradicts the above assumption.

According to the above analysis, we know that we cannot find two connections in the network such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$, based on previous policies with the assumption of one wavelength in one direction. Thus, under this condition, the network is one-OAF

diagnosable.

Next, we need to prove that a multi-wavelength network can be one-OAF diagnosable for each wavelength if there is no wavelength converter.

Although there are multiple wavelengths in the whole network, according to our crosstalk attack model, the crosstalk attack connection can only affect the same wavelength connections at the wavelength selective switches. Therefore, a crosstalk attack on one wavelength does not have any affect on the normal connections on other wavelengths. We have already shown that we can diagnose all connections on one wavelength. Therefore, we can always detect OAFs on all wavelengths in the whole network, if there is only one OAF on each wavelength.

In conclusion, as long as there is no more than one OAF on each wavelength and there is no wavelength converter in whole network, we can always localize the OAFs based on our models and policies. □

5.2.1.2 Examples

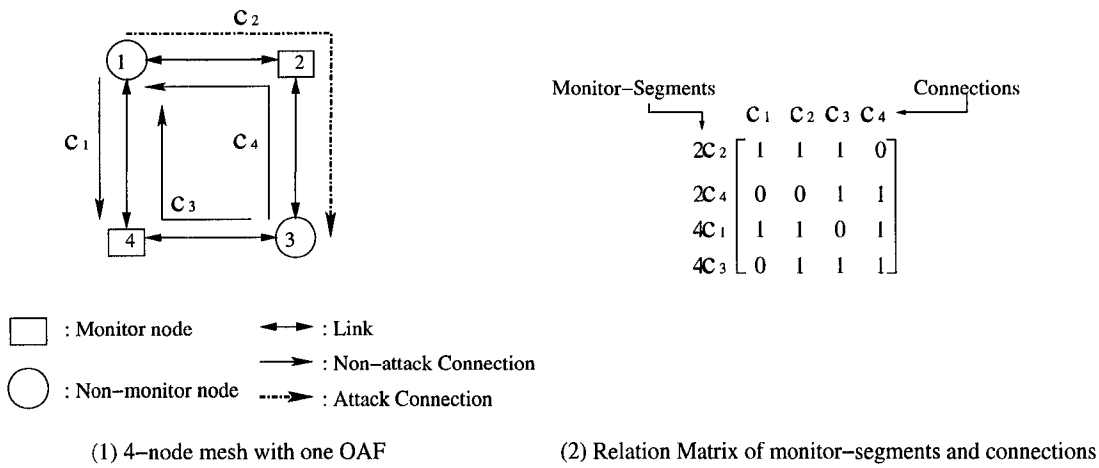
Figure 5.1 (1) depicts a 4-node bi-directional mesh network. According to sparse monitor placement policy, two monitor nodes are necessary in this network. Here, we choose nodes 2 and 4 as the monitor nodes and nodes 1 and 3 as non-monitor nodes. By considering that attack connections can only affect connections in same wavelength, to simplify our example, we assume that only one wavelength is supported in this network.

Suppose we have some normal connections and only one of them is a OAF.

The current normal connection set is:

$Normal\ connection\ set = \{c_1(1 \rightarrow 4),\ c_2(1 \rightarrow 2 \rightarrow 3),\ c_3(3 \rightarrow 4 \rightarrow 1),\ c_4(3 \rightarrow 2 \rightarrow 1)\}$.

For each non-monitor node one normal connection exists from this node to every of its OHMs, thus according to our test connection setup policy, no test connection is



(1) 4–node mesh with one OAF (2) Relation Matrix of monitor–segments and connections

Figure 5.1 Diagnose the OAF in the network without test connection

necessarily needed.

Thus, the current monitor-segment set is $msc = \{2c_2, 2c_4, 4c_1, 4c_3\}$, and the relation matrix between these monitor-segments and the connections is shown in Figure 5.1 (2).

Let us assume that connection $\{c_2(1 \rightarrow 2 \rightarrow 3)\}$ is the OAF. Then, we can get the status of all monitor-segments immediately: $S(2c_2) = A = 1$, $S(2c_4) = \bar{A} = 0$, $S(4c_1) = A = 1$, and $S(4c_3) = A = 1$. Thus, $\overrightarrow{S(msc)}$ can be obtained as:

$\overrightarrow{S(msc)} = (S(2c_2)\ S(2c_4)\ S(4c_1)\ S(4c_3)) = (1\ 0\ 1\ 1)$.

Then, vector $\overrightarrow{S(c)}$ can be obtained as:

$$\begin{aligned}
\overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) & S(c_4) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}.
\end{aligned}$$

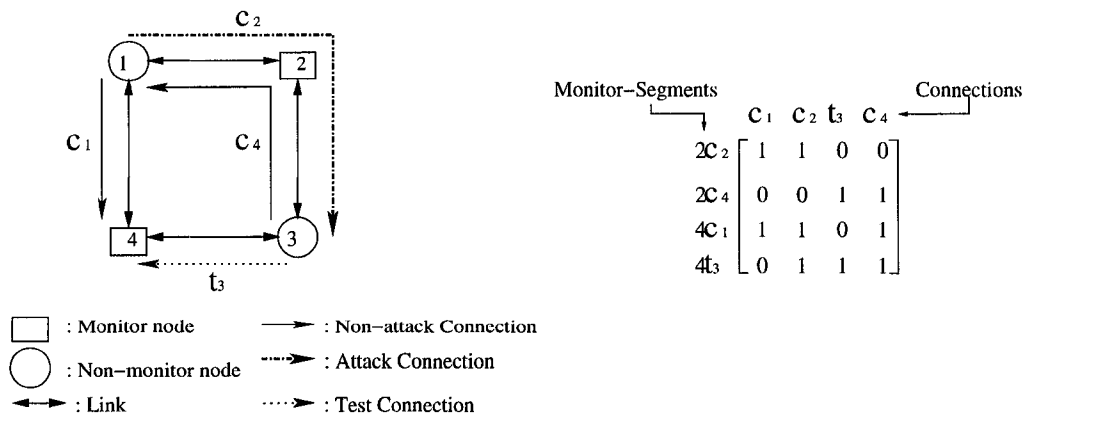
All $S(c_1)$, $S(c_3)$, and $S(c_4)$ are greater than 0, which means connections c_1, c_3, and

c_4 are all IFs, while $S(c_2) = 0$, which means that c_2 is in $UnIdentified$ status. Thus, the only $UnIdentified$ connection c_2 must be OAF.

Now, let us assume that connection c_3 does not exist. Then, according to our test connection setup policy, a test connection t_3 is established from node 3 to node 4 because of a lacking monitor-segment on link (3, 4), as shown in Figure 5.2 (1). Then, as shown in Figure 5.2 (2), we can get the relation matrix of monitor-segments and connections. By using the same method shown in previous example, we get:

$$\begin{aligned}
\overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & S(c_2) & S(t_3) & S(c_4) \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}.
\end{aligned}$$

Still, we can determine the only UnIdetified connection c_2 as the OAF.



(1) one test connection be setup in 4-node network (2) Relation Matrix of monitor-segments and connections

Figure 5.2 Diagnose the OAF in the network with a test connection

These two examples tell us that test connections will not utilize much of the resources

in the network. According to our test connection setup policy, a test connection is needed only if there is no monitor-segment on one link. If a test connection cannot be set because there are no spare resources on a certain link, then the resources must be used by another connection, which can be used as monitor-segment. Thus, test connections will not affect the network throughput.

Now, let us consider two crosstalk attack connections on two different wavelengths, as shown in Figure 5.3. In this example, there are two wavelengths λ_1 and λ_2 in the network, and we use two panels to represent them. There is one attack connection on each wavelength, connection $\{1 \rightarrow 2\}$ on λ_1 and connection $\{1 \rightarrow 4\}$ on λ_2. We can easily use the above matrix calculation to determine that these two connections are crosstalk attack. Because there is only one crosstalk attack on each wavelength, and a crosstalk attack on λ_1 cannot affect connections on λ_2, our method has already located the malicious connections in the network.

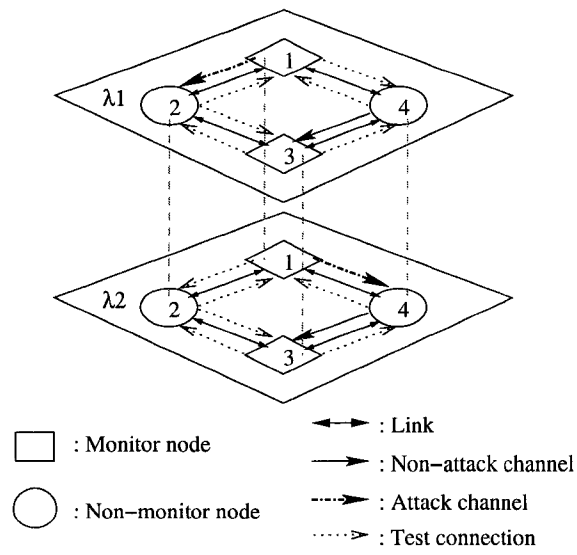


Figure 5.3 Two attack connections on different wavelength

5.2.2 Sparse Monitoring Policy II

The previous method still needs a lot of monitor nodes in a network. For example, almost half of the nodes in a mesh network are required to be monitors. To reduce the total number of monitor nodes in a network, another method is proposed. With this new method, fewer monitors are required in the whole AON.

5.2.2.1 Description of Policy II

1. **Monitor placement policy**

   Any non-monitor node u must have at least one OHM.

2. **Test Connection Setup Policy**

   For any monitor or non-monitor node, if there is a normal connection passing through or terminating at this node, one test connection from this node to each OHM (if existing) is needed if no normal connection exists on the corresponding link.

3. **Routing policy**

   (a) For any arbitrary pair of connections c_i and c_j, if neither source node is a monitor node, then, $U(c_i) \neq U(c_j)$ should be always satisfied;

   (If $\forall c_i,\ c_j \in R$, $U(c_i) = \{u_i, \dots\}$, $U(c_j) = \{u_j, \dots\}$, and $u_i, u_j \notin M$, then $U(c_i) \neq U(c_j)$.)

   (b) for any arbitrary pair of connections c_i and c_j which share at least one node u, if neither source node is a monitor node, then at least one of following conditions should be satisfied:

   (If $\forall c_i,\ c_j \in R$, $U(c_i) = \{u_i, \dots\}$, $U(c_j) = \{u_j, \dots\}$, $u_i, u_j \notin M$, and $u \in \{U(c_i) \cap U(c_j)\}$ then:)

i. u is a monitor node, or

($u \in M$, or)

ii. either $UNN(u, c_i)$ or $UNN(u, c_j)$ should be a monitor node, or

($\{UNN(u, c_i) \cup UNN(u, c_j)\} \subseteq M$, or)

iii. at least one node v, $v \in U(c_i)$ but $v \notin U(c_j)$, exists, such that $DNN(v, c_i) \in M$ exists or one of its OHM $m \notin U(c_i)$ exists.

($\exists v \in U(c_i)$ but $v \notin U(c_j)$, $DNN(v, c_i) \in M$ or $\exists m \in M$, $m \in OHM(v)$, and $m \notin U(c_i)$.)

(c) normally we use the shortest path algorithm except for as in the above cases.

Comparing this policy with the previous Sparse Monitor Policy I where any non-monitor node u requires $D(u)$ OHMs, we see that this new method only requires one OHM for each non-monitor node. Considering the expense of a monitor, this is a big advantage.

Claim 2: With the above new sparse monitoring policies, a network is one-OAF diagnosable.

Proof. With a given network denoted by graph $G(V, E)$, let M denote the set of monitor nodes, and let N denote the set of non-monitor nodes, $M \subseteq V$, $N \subset V$, and $M \bigcup N = V$. Let C denote the set of connections in the network. Let $c_i \in C$ be a connection consisting of node $\{u_0, u_1, u_2, \ldots, u_k, \ldots\}$. Let $U(c_i)$ denote the set of nodes on connection c_i's path.

First, in each link, we assume there is only one wavelength on each direction.

1. According to the monitor placement policy, for a non-monitor node at least one of its neighbor nodes should be a monitor node, and according to the test connection setup policy, if there is a connection traversing or terminating at a non-monitor node, then there must be a monitor-segment between this node and each of its

OHMs. Thus, for one connection c, at least one monitor-segment monitors it, i.e., $\Gamma^{-1}(c) \neq \emptyset$ is satisfied $\forall c \in C$.

2. The necessary and sufficient condition for an one-OAF diagnosable network is that any arbitrary pair of connections, c_i and c_j, should satisfy $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. Now, suppose there exist two connection c_i and c_j such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$. For any arbitrary pair of connections, only one of following possibilities can be true.

   (a) At least one of them originates from a monitor node. Without loss of generality, we assume that c_i originates from monitor m. According to monitor-segment property I, any connection originating from a monitor can make a special monitor-segment that only monitors this connection. Thus, a monitor-segment mc_i made by c_i and m does not monitor other connections including c_j (i.e., $mc_i \in \Gamma^{-1}(c_i)$) and $mc_i \notin \Gamma^{-1}(c_i)$. Therefore, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$, which contradicts the above assumption.

   (b) None of these connections originates from a monitor node. Then, there are two possible cases.

      i. $U(c_i) \cap U(c_j) = \emptyset$: the connections do not share any nodes between them. Then, without loss of generality, assume $\exists v \in U(c_i)$ but $\notin U(c_j)$, then one monitor-segment $msc_{(v \to m)}$ made by node v and one of its OHMs m exists. Because $msc_{(v \to m)} \in \Gamma^{-1}(c_i)$ but $\notin \Gamma^{-1}(c_j)$, $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$. This contradicts the above assumption.

      ii. $U(c_i) \cap U(c_j) \neq \emptyset$. Assume $u \in (U(c_i) \cap U(c_j))$. According to the routing policy, only three scenarios can be allowed:

         A. Node u is a monitor node. Then, because u cannot be the source node for both connections, either $UNN(u, c_i)$ or $UNN(u, c_j)$ must exist. Without loss of generality, assume $UNN(u, c_i)$ exists. Then,

monitor-segment $msc_{(UNN(u,c_i)\rightarrow u)}$, made by $(UNN(u,c_i) \rightarrow u)$ and monitor node u, should be in $\Gamma^{-1}(c_i)$. Because there is only one wavelength in each direction, $UNN(u,c_i) \neq UNN(u,c_j)$. According to our monitor-segment definition, $msc_{(UNN(u,c_i)\rightarrow u)} \notin \Gamma^{-1}(c_j)$, which means $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$: this contradicts the above assumption.

B. $UNN(u,c_i)$ or $UNN(u,c_j)$ is a monitor node. Without loss of generality, assume $UNN(u,c_i) \in M$ exists. Then, for same reason as above, $UNN(u,c_i) \neq UNN(u,c_j)$, and monitor-segment $msc_{(u\rightarrow UNN(u,c_i))} \in \Gamma^{-1}(c_j)$ but $\notin \Gamma^{-1}(c_i)$, which means $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$: this again contradicts the above assumption.

C. Node v is only in either $U(c_i)$ or $U(c_j)$, but not both. Without loss of generality, assume $v \in U(c_i)$. According to routing policy, either $DNN(v,c_i) \in M$ exists or for one of its OHM $m \notin U(c_i)$ should be true. If $DNN(v,c_i) \in M$ exists, then monitor-segment $msc_{(v\rightarrow DNN(v,c_i))} \in \Gamma^{-1}(c_i)$, and since $v \notin U(c_j)$, according to the monitor-segment definition, $msc_{(v\rightarrow DNN(v,c_i))} \notin \Gamma^{-1}(c_j)$, which means $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$: this contradicts the above assumption. If for one of v's OHM $m \notin U(c_i)$ is true, then monitor-segment $msc_{(v\rightarrow m)} \in \Gamma^{-1}(c_i)$. For the same reason, $msc_{(v\rightarrow m)} \in \Gamma^{-1}(c_j)$, which means $\Gamma^{-1}(c_i) \neq \Gamma^{-1}(c_j)$: this also contradicts the above assumption.

According to the above analysis, we know that we cannot find two connections in the network such that $\Gamma^{-1}(c_i) = \Gamma^{-1}(c_j)$ based on previous policies, with the assumption of one wavelength per direction. Thus, under this condition, the network is one-OAF diagnosable.

Next, we need to prove that a multi-wavelength network can be one-OAF diagnosable for each wavelength if there is no wavelength converter.

Although there are multiple wavelengths in the whole network, according to our crosstalk attack model, the crosstalk attack connection can only affect the same wavelength connections at the wavelength selective switches (*homowavelength* feature). Therefore, a crosstalk attack on one wavelength does not have any chance to affect the normal connections on other wavelengths. We have already showed that we can diagnose all connections on one wavelength. Therefore, we can always detect OAFs on all wavelengths in the whole network, if there is only one OAF on each wavelength.

In conclusion, as long as there is no more than one OAF on each wavelength and there is no wavelength converter in whole network, we can always localize the OAFs based on our models and policies. □

5.2.2.2 Connection Routing Algorithm in One-OAF Networks

In this section we develop one practical routing algorithm. Without loss of generality, we develop a variant of the shortest-path algorithm that satisfies the above routing constrains.

The pseudo code for the algorithm is given below.

BEGIN:

Given a node request.

Run Shortest-Path-Algorithm to find the source-destination path. /*Test connections are ignored to compute the path and removed if the path uses those links with the test connections*/

IF Fail to find any available path, reject this request,

ELSE find one path P1,

IF source node s is a monitor node,

THEN accept this request and setup this connection with path P1.

ELSE source node s is a non-monitor node,

Check number of nodes n on P1,

IF $n \geq 3$,

THEN accept this request and setup this connection with path P1.

ELSE check all existing connections originated from s,

IF all existing connections' paths include at least 3 nodes,

THEN accept this request and setup this connection with path P1.

ELSE remove one link on path P1 from original graph and reiterate the algorithm.

ENDIF

ENDIF

ENDIF

ENDIF

END

Suppose the maximum output degree of network nodes is $Max\{D(u)\} = d_N$, then, with this routing algorithm, at most d_N connections need to be checked before we can make decision for the connection request.

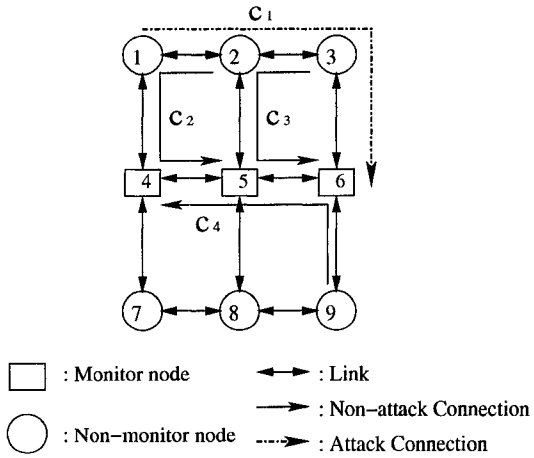
5.2.2.3 Example

Figure 5.4 (1) depicts a 9-node bi-directional mesh network. According to the sparse monitor placement policy, only three monitor nodes are necessary in this network. Here, we choose nodes 4, 5, and 6 as the monitor nodes and the remaining nodes as non-monitor nodes. By considering attack connections which are homowavelength, to simplify our example, we assume that only one wavelength is supported in this network.

Suppose we have some normal connections and only one of them is a OAF.

The current normal connection set is:

Normal connection set = $\{c_1(1 \rightarrow 2 \rightarrow 3 \rightarrow 6),\ c_2(2 \rightarrow 1 \rightarrow 4 \rightarrow 5),\ c_3(3 \rightarrow 2 \rightarrow 5 \rightarrow 6),\ c_4(9 \rightarrow 6 \rightarrow 5 \rightarrow 4)\}$.



(1) 9–node mesh with one OAF

Monitor–Segments — Connections

	c_1	c_2	c_3	c_4
$4c_2$	1	1	0	0
$4c_4$	0	0	1	1
$5c_3$	1	1	1	0
$5c_4$	1	0	0	1
$6c_1$	1	0	1	0
$6c_3$	0	1	1	0
$6c_4$	0	0	0	1

(2) Relation Matrix of monitor–segments and connections

Figure 5.4 Homowavelength crosstalk attack diagnosable network

According to our test connection setup policy, no test connection is necessarily needed. Thus, the current monitor-segment set is: $msc = \{4c_2, 4c_4, 5c_3, 5c_4, 6c_1, 6c_3, 6c_4\}$, and the relation matrix between these monitor-segments and the connections is shown in Figure 5.4 (2).

Let us assume that connection $\{c_1(1 \rightarrow 2 \rightarrow 3 \rightarrow 6)\}$ is the OAF. Then, we can get the status of all monitor-segments immediately: $S(4c_2) = A = 1$, $S(4c_4) = \bar{A} = 0$, $S(5c_3) = A = 1$, $S(5c_4) = A = 1$, $S(6c_1) = A = 1$, $S(6c_3) = \bar{A} = 0$, and $S(6c_4) = \bar{A} = 0$. Thus, $\overrightarrow{S(msc)}$ can be obtained as:

$\overrightarrow{S(msc)} = (S(4c_2)\ S(4c_4)\ S(5c_3)\ S(5c_4)\ S(6c_1)\ S(6c_3)\ S(6c_4)) = (1\ 0\ 1\ 1\ 1\ 0\ 0)$.

Then, vector $\overrightarrow{S(c)}$ can be obtained as:

$$\overrightarrow{S(c)} = \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) & S(c_4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}.$$

All values of $S(c_2)$, $S(c_3)$, and $S(c_4)$ are greater than 0, which means connections c_2, c_3, and c_4 are all IFs, while $S(c_1) = 0$, which means that c_1 is in UnIdentified status. Thus, the only UnIdentified connection c_1 must be OAF.

5.3 Sparse Monitoring Policies for More than One OAF

The previous section provides the policies for One-OAF diagnosable networks, but how to place the monitors and set up test connections for more than one OAF is still an open question. Since increasing numbers of possible $OAFs$ in a network necessitate increasingly complicated algorithms, only a 2-OAF diagnosable network is discussed in this section. First we propose a sparse monitoring scheme, which includes monitor placement as well as regular and test connection setting policies, then we prove that any network using such method is 2-OAF diagnosable.

5.3.1 Sparse Monitoring Policy for 2-OAF Network

1. **Monitor placement policy**

To guarantee the exact location of the OAFs in a network, we propose the following sparse monitor placement policy:

(a) a non-monitor node u must have $D(u)$ OHMs;

(b) a node u with a pendant node as its neighbor must be a monitor node.

2. **Test Connection Setup Policy**

We assume that each link in the network is bi-directional so that there is a fiber for each direction in each link. According to our monitoring mechanism, there are two kinds of connections: *normal connections* which are set up by users, and the *test connections* which are requested by the network management system. Establishing test connections is an important step in determining if a node is a PAN or not. We use the following rules to set up test connections.

Test Connection Set Up:

For a non-monitor node u, if there is a normal connection c on wavelength λ passing through or terminating at u, one test connection from node u to each OHM, except u's up-stream neighbor node $UNN(u, c)$, is needed if no normal connection provides a monitor-segment on the corresponding link.

3. **Routing policy**

To guarantee the exact location of the OAFs in a network, we use the following rule to set up a connection.

(a) If a connection c_i's source is a non-monitor node that is also on another connection c_j's path, then, c_i must pass through three continuous nodes $(n_1, n_2, n_3) \not\subseteq U(c_j) \cup U(c_k)$, where $c_k \neq c_i, c_j$ is an arbitrary connection in the network.

$(\forall c_i,\ c_j, c_k \in C, U(c_i) = \{u_i, \dots\}$, and $u_i \in U(c_j)$, then, $\exists\{n_1, n_2, n_3\} \subset U(c_i)$ but $(n_1, n_2, n_3) \not\subseteq \{U(c_j) \cup U(c_k)\}$.)

(b) Otherwise, any path selection algorithm, such as shortest path algorithm, can be used.

According to our crosstalk attack model, the crosstalk attack only affects the same wavelength connection at the wavelength selective switch. To simplify our analysis, in the following parts we assume that there is no wavelength converter in the whole network, and for each link, only one fiber exists in each direction.

In the following, we prove that a network is always 2-OAF diagnosable if it is designed using the models and policies described above.

Lemma 6: If a connection c_i passes through 3 continuous nodes that are not in $U(c_j)$, then there is at least one monitor segment msc_i such that $msc_i \in \Gamma^{-1}(c_i)$, but $msc_i \notin \Gamma^{-1}(c_j)$.

Proof. Without loss of generality, assume that the 3 continuous nodes are $\{n_1, n_2, n_3\}$ in the direction of c_i. Because of the above monitor placement policy, if n_2 is a non-monitor node, then both n_1 and n_3 must be monitor nodes, otherwise, n_2 must be a monitor node. If n_2 is not a monitor node, then according to definition, monitor segment $msc_i = (n_2 \rightarrow n_3) \in \Gamma^{-1}(c_i)$ but not in $\Gamma^{-1}(c_j)$: this lemma holds. If n_2 is a monitor node, since both n_1 and n_2 are not in $U(c_j)$, then monitor segment $msc_i = (n_1 \rightarrow n_2) \in \Gamma^{-1}(c_i)$, but not in $\Gamma^{-1}(c_j)$. Thus the lemma holds.

□

Claim 3: With the above monitor placement, test connection setup, and routing policies, a network with one fiber on each link and without any wavelength converters is 2-OAF diagnosable on each wavelength.

Proof. With a given network denoted by graph $G(V, E)$, let M denote the set of monitor nodes, and let N denote the set of non-monitor nodes, $M \subseteq V$, $N \subset V$, and $M \bigcup N = V$. Let $C = R \bigcup T$ denote the set of connections in the network, where R is the regular set of connections, and T is the set of test connections. Let $U(c_i)$ denote the set of nodes on connection c_i's path.

First, in each link, we assume there is only one wavelength in each direction.

1. According to the sparse monitor placement policy, each neighboring node of a non-monitor node must be a monitor node, which means on each link at least one node is a monitor node. Thus, for one connection c, at least one monitor node $m \in U(c)$. According to the definition of monitor-segment, at least one monitor-segment monitors this connection (i.e., $\Gamma^{-1}(c) \neq \emptyset$ holds $\forall\ c \in C$).

2. According to Theorem 3, for any three arbitrary connections c_i, c_j, and c_k, the necessary and sufficient condition for an 2-OAF diagnosable network is $\Gamma^{-1}(c_i) \nsubseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. Now, suppose $\Gamma^{-1}(c_i) \subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$, then there are two possibilities.

   (a) c_i's source node is a non-monitor node. Then, there are two possible cases.

      i. Connection c_i's source node $n_i \notin U(c_j) \cup U(c_k)$. Because at least one monitor exists on each link, $DNN(n_i, c_i)$ must be a monitor node. Let $m_i = DNN(n_i, c_i)$. Since $n_i \notin U(c_j) \cup U(c_k)$, monitor-segment $m_i c_i$ can only monitor connection c_i, thus, $\Gamma^{-1}(c_i) \nsubseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. This contradicts the above assumption.

      ii. $n_i \in U(c_j) \cup U(c_k)$. Without loss of generality, suppose $n_i \in U(c_j)$. According to routing policy, connection c_i should pass three continuous nodes that are not in $U(c_j) \cup U(c_k)$. According to lemma 4, there is

always a monitor-segment $msc_i \notin \Gamma^{-1}(c_j)$ as well as $msc_i \notin \Gamma^{-1}(c_k)$, thus $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$. This again contradicts the above assumption.

(b) c_i's source node is a monitor node. According to previous discussion concerning special cases of monitor-segments, any connection originating from a monitor can make up a special monitor-segment that would only monitor this connection. Thus, a monitor-segment msc_i made up by c_i and m does not monitor other connections including c_j and c_k (i.e., $msc_i \in \Gamma^{-1}(c_i)$ and $msc_i \notin \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$). $\Gamma^{-1}(c_i) \not\subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$: this contradicts the above assumption.

From the above analysis, we know that we cannot find three connections in the network such that $\Gamma^{-1}(c_i) \subseteq \Gamma^{-1}(c_j) \cup \Gamma^{-1}(c_k)$ based on previous policies, with the assumption of one wavelength on one direction. Thus, under this condition, the network is 2-OAF diagnosable.

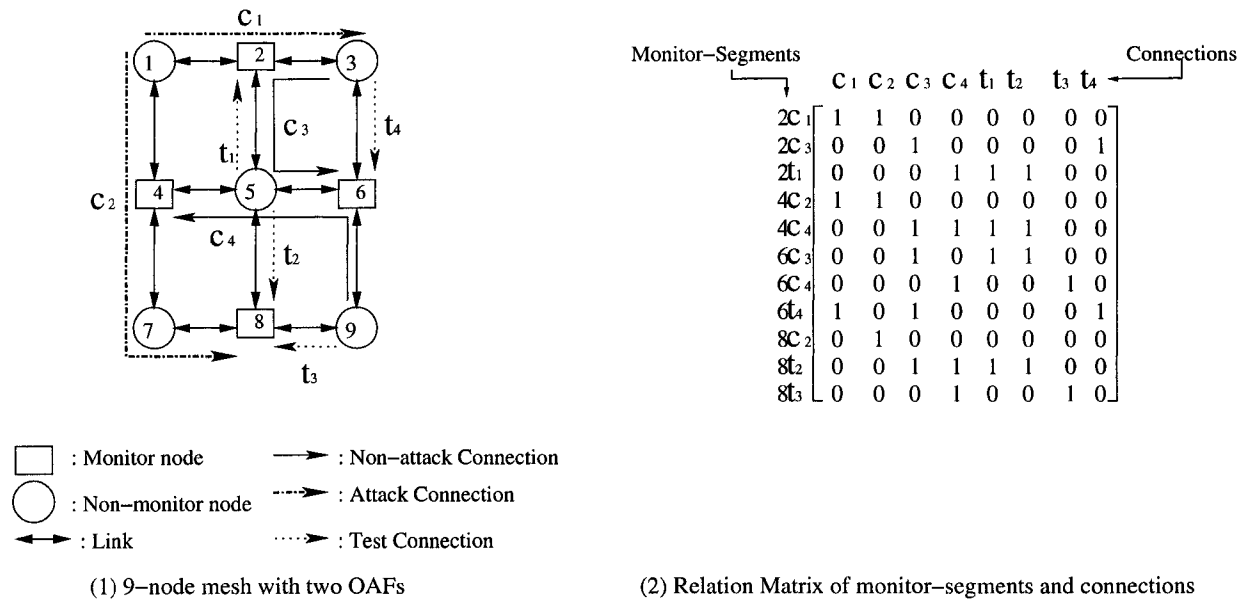
In case of a multi-wavelength network, although there are multiple wavelengths in the whole network, according to our crosstalk attack model, the crosstalk attack connection can only affect the same wavelength connections at the wavelength selective switches. Therefore, a crosstalk attack on one wavelength does not have any affect on the normal connections on other wavelengths. We have already shown that we can diagnose all connections on one wavelength. Therefore, we can always detect OAFs on each wavelength in the whole network, as long as there are no more than 2 OAFs on each wavelength.

□

5.3.2 Examples

Figure 5.5 (1) depicts a 9-node bi-directional mesh network. In this example, this network is a $2-OAF$ diagnosable network. According to our sparse monitor placement

policy, four monitor nodes are necessary in this network. Here, we choose nodes 2, 4, 6, and 8 as the monitor nodes, and the rest nodes as non-monitor nodes. By considering that attack connections can only affect connections in same wavelength, to simplify our example, we assume that only one wavelength is supported in this network.



(1) 9–node mesh with two OAFs

(2) Relation Matrix of monitor–segments and connections

Figure 5.5 Diagnose 2 OAFs in a network

Suppose we have some normal connections, two of which are OAFs.

The current normal connection set is

Normal connection set = $\{c_1(1 \rightarrow 2 \rightarrow 3),\ c_2(1 \rightarrow 4 \rightarrow 7 \rightarrow 8),\ c_3(3 \rightarrow 2 \rightarrow 5 \rightarrow 6),\ c_4(9 \rightarrow 6 \rightarrow 5 \rightarrow 4)\}$.

According to our test connection setup policy, for each non-monitor node at least one normal connection or one test connection must exist from this node to each of its OHMs, therefore the test connection set is

Test connection set = $\{t_1(5 \rightarrow 2),\ t_2(5 \rightarrow 8),\ t_3(9 \rightarrow 8)\ \ t_4(3 \rightarrow 6)\}$.

Thus, the current monitor-segment set is

$$msc = \{2c_1, 2c_3, 2t_1, 4c_2, 4c_4, 6c_3, 6c_4, 6t_4, 8c_2, 8t_2, 8t_3\}$$

and the relation matrix between these monitor-segments and the connections is shown in Figure 5.5 (2).

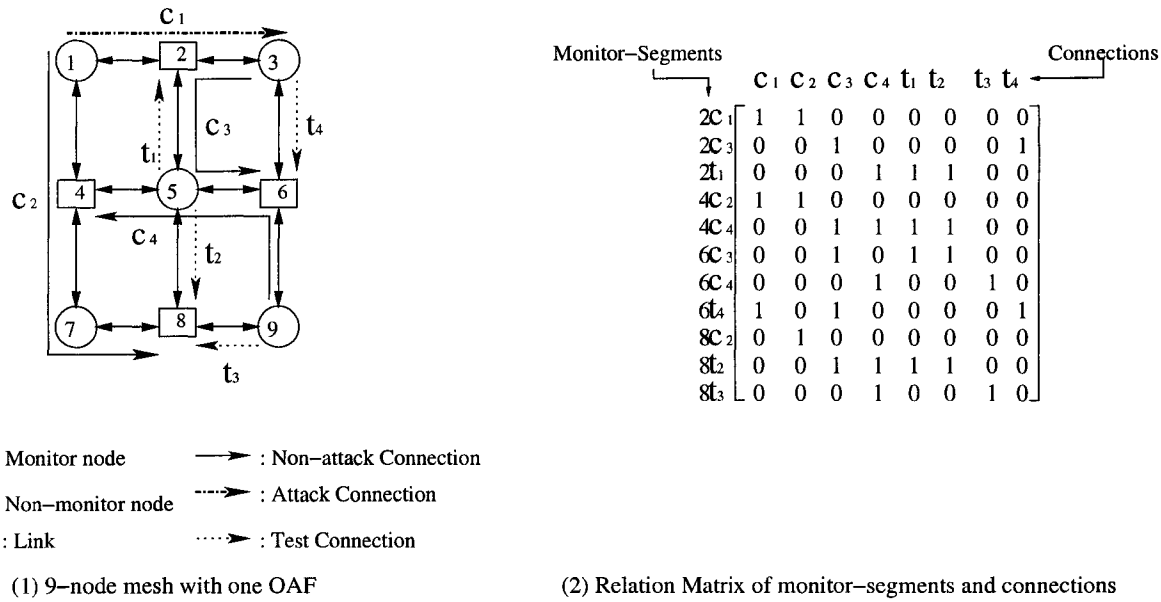
Let us assume that connections $\{c_1(1 \rightarrow 2 \rightarrow 3)\}$ and $\{c_2(1 \rightarrow 4 \rightarrow 7 \rightarrow 8)\}$ are OAFs. Then, we can get the status of all monitor-segments immediately: $S(2c_1) = A = 1$, $S(2c_3) = \bar{A} = 0$, $S(2t_1) = \bar{A} = 0$, $S(4c_2) = A = 1$, $S(4c_4) = \bar{A} = 0$, $S(6c_3) = \bar{A} = 0$, $S(6c_4) = \bar{A} = 0$, $S(6t_4) = A = 1$, $S(8c_2) = A = 1$, $S(8t_2) = \bar{A} = 0$, and $S(8t_3) = \bar{A} = 0$. Thus, $\overrightarrow{S(msc)}$ is obtained as

$$\begin{aligned}\overrightarrow{S(msc)} &= (\ S(2c_1)\ \ S(2c_3)\ \ S(2t_1)\ \ S(4c_2)\ \ S(4c_4) \\ &\qquad S(6c_3)\ \ S(6c_4)\ \ S(6t_4)\ \ S(8c_2)\ \ S(8t_2)\ \ S(8t_3)\ ) \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.\end{aligned}$$

Then, vector $\overrightarrow{S(c)}$ is obtained as

$$\begin{aligned}\overrightarrow{S(c)} &= \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) & S(c_4) & S(t_1) & S(t_2) & S(t_3) & S(t_4) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.\end{aligned}$$

$S(c_3)$, $S(c_4)$, $S(t_1)$, $S(t_2)$, $S(t_3)$, and $S(t_4)$ are greater than 0, which means connections c_3, c_4, t_1, t_2, t_3, and t_4 are all IFs. Since $S(c_1) = 0$ and $S(c_2) = 0$, it implies that both c_1 and c_2 are in UnIdentified status. Thus, according to Corollary 2, the UnIdentified connections c_1 and c_2 must be OAFs.



(1) 9-node mesh with one OAF (2) Relation Matrix of monitor-segments and connections

Figure 5.6 Diagnose 1 OAF in a network

Now, let us assume that only connection c_1 is OAF in the same network, as shown in Figure 5.6. Because the sets of connections are the same in both cases, monitor-segment set and the relation matrix will be the same as the previous example. Because we assume that connection $\{c_1(1 \rightarrow 2 \rightarrow 3)\}$ is an OAF, then we can get the status of all monitor-segments immediately: $S(2c_1) = A = 1$, $S(2c_3) = \bar{A} = 0$, $S(2t_1) = \bar{A} = 0$, $S(4c_2) = A = 1$, $S(4c_4) = \bar{A} = 0$, $S(6c_3) = \bar{A} = 0$, $S(6c_4) = \bar{A} = 0$, $S(6t_4) = A = 1$, $S(8c_2) = \bar{A} = 0$, $S(8t_2) = \bar{A} = 0$, and $S(8t_3) = \bar{A} = 0$. Thus, $\overrightarrow{S(msc)}$ is obtained as

$$\begin{aligned}\overrightarrow{S(msc)} &= (S(2c_1) \;\; S(2c_3) \;\; S(2t_1) \;\; S(4c_2) \;\; S(4c_4) \\ &\qquad S(6c_3) \;\; S(6c_4) \;\; S(6t_4) \;\; S(8c_2) \;\; S(8t_2) \;\; S(8t_3)) \\ &= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.\end{aligned}$$

Then, vector $\overrightarrow{S(c)}$ is obtained as

$$\overrightarrow{S(c)} = \begin{pmatrix} S(c_1) & S(c_2) & S(c_3) & S(c_4) & S(t_1) & S(t_2) & S(t_3) & S(t_4) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

$S(c_2)$, $S(c_3)$, $S(c_4)$, $S(t_1)$, $S(t_2)$, $S(t_3)$, and $S(t_4)$ are greater than 0, which means connections c_2, c_3, c_4, t_1, t_2, t_3, and t_4 are all IFs. Since $S(c_1) = 0$, it implies that only c_1 is in UnIdentified status. Thus, according to corollary 2, the UnIdentified connection c_1 must be the OAF.

CHAPTER 6 CONCLUSION AND FUTURE WORK

6.1 Conclusion

In this dissertation, we have discussed the physical security problems in an AON. Among all possible malicious attacks, we mainly focused on crosstalk attacks because its propagation capability can cause more harm than other kind of attacks. We studied the physical origination of crosstalk attack and its features and compared several available optical signal detection techniques. Then, we established a crosstalk attack model as well as a monitor model. Based on these models, the monitor-segment concept was developed and a necessary and sufficient condition for one-crosstalk-attack diagnosable network was given and proven. Next, we extended this result and proved the necessary and sufficient condition for a more than one crosstalk attack diagnosable network. To implement such diagnosable network, we developed several sparse monitoring algorithms for a one-crosstalk-attack diagnosable AON and a general case k-crosstalk-attack diagnosable AON, respectively.

Based on our research, we draw the following conclusions:

1. It is possible to design diagnosable network with sparse monitoring as long as appropriate routing and test connection strategies are followed. The necessary and sufficient conditions for one-crosstalk-attack and k-crosstalk-attack diagnostic networks have been proved in this dissertation.

2. For a mesh network, less than half the nodes need to be monitor nodes to satisfy

one-OAF diagnostic purpose, and about half of the nodes need to be monitor nodes to satisfy 2-OAF diagnostic purpose. Considering the fact that the monitor devices are expensive, this really provides a big advantage.

3. The complexity of our diagnosis algorithms is $O((|M| \times d_M)^2 \times |C|)$. Here $|M|$is the total number of monitors in a network, d_M is the maximum degree of all monitor nodes, and $|C|$ is the total number of connections in the network. All operations needed in the computation are $+$ and $\oplus$. Hence, these methods are scalable.

4. Our algorithms need setting up test connections. These test connections will not utilize much resources in the network. According to our test connection setup policy, a test connection is needed only if there is no monitor-segment on a link. If a test connection cannot be setup because there are no spare resources in a certain link, it must be because that the resources are being used by another connection, which can be used as the monitor-segment. Thus, test connections will not affect the network throughput.

6.2 Impact of Our Contributions

Today's all-optical networks provide extremely limited attack management capability. Although optical networking is one of the fastest growing areas in networking, even theoretical attack management research in the optical domain only skims the surface. Because the transparency characteristic of AONs means that data does not undergo optical-to-electrical or electrical-to-optical conversion, AONs introduce new physical layer mechanisms that change potential models of attack from those that are well known for traditional electronic networks. Thus, many security vulnerabilities that do not exist in traditional networks will occur in AONs. In a network without regeneration ability, a malicious connection, i.e., a crosstalk attack, can propagate from its primary source

to other nodes without losing its attack capability. This makes attacks detection and localization become much more difficult, and high data rates characteristic makes things much worse because even a very short time service disturbance means a huge data loss. To come up with a fast attack-diagnostic technique is extremely important for a AON management system.

Among all possible attack methods, the crosstalk attack has the highest damage capabilities. The work presented in this dissertation is a pioneering effort on the research in the area of crosstalk attack in AON. Since no prior work exists on complete modeling and analysis of crosstalk attacks using sparse monitoring, we, for the first time, have developed a complete crosstalk attack model, which includes the crosstalk attack's propagation feature. Moreover, we have also developed a monitor model for the detection purpose based on current available detection techniques and reasonable assumptions. We also developed a complete diagnosis algorithm to detect and locate the attack sources.

The results of this research will enable us to design better and more efficient fault and attack tolerant optical fiber based network. Since the society is very dependent on fully functional computing and networking system, our research will have significant economic impact as well.

6.3 Future Work

The research reported in this dissertation can be extended in several different ways. The models we presented in Chapter 3 only focus on crosstalk attack. However, crosstalk attack may not be the only security problem that occurs in an AON. Other attacks, such as eavesdropping and correlated jamming attack, can happen in the network. More studies are required to understand the behavior of these attacks. Those attack models need to be established. Moreover, we assumed that the only attack that occurs in an

AON is the crosstalk attack described in Chapter 3. This assumption is not valid in the strict sense because different attacks can occur in the same network simultaneously. A more complex and flexible model may be developed if different attacks are considered in the same network.

The necessary and sufficient conditions we proved in Chapter 4 are only valid for diagnosing crosstalk attacks only. A possible direction is to extend these conditions to be valid for diagnosing possible co-existing different attacks.

Using sparse monitors to diagnose possible corsstalk attack is a new concept in the literature. However, only heuristic solutions for placing monitors and routing for one-OAF and k-OAF diagnostic AON have been proposed in Chapter 5. More sophisticated analysis for the monitor placement policy, the test setup policy, and the corresponding routing policy need to be studied. Evaluation of the AON performance using different policies must also be investigated. A precise and comprehensive network cost model would be useful to determine an optimal solution.

BIBLIOGRAPHY

[1] R. C. Alferness. The all-optical networks. *WCC - ICCT 2000*, 1:14–15, August 2000.

[2] R. C. Alferness. The all-optical networks. *WCC - ICCT 2000*, 1:14–15, August 2000.

[3] A. Amrani, J. Roldan, and G. Junyent. Optical monitoring system for scalable all-optical networks. *Proceeding of IEEE LEOS '97 10th Annual Meeting*, 2:270–271, November 1997.

[4] William T. Anderson, Janet Jackel, G.-K. Chang, and Hongxing Dai etc. The monet project-a final report. *IEEE Journal of Lightwave Technology*, 18(2):1988–2009, December 2000.

[5] R. Antosik. Protection and restoration in optical networks. *2nd International Conference on Transparent Optical Networks*, 2000.

[6] Ruth Bergman, Muriel Medard, and Serena Chan. Distributed algorithms for attack localization in all-optical networks. *Network and Distributed System Security Symposium*, 1998.

[7] Bob Chomycz. *Fiber Optic Installer's Field Manual.* McGraw-Hill, 2000.

[8] G. Conte, M. Listanti, M. Settembre, and R. Sabella. Strategy for protection and restoration of optical paths in wdm backbone networks for next-generation internet infrastructures. *Journal of Lightwave Technology*, 20(8):1264–1276, August 2002.

[9] J. A. Copeland and R. C. Garcia. Real-time anomaly detection using soft-computing techniques. *IEEE Proceedign of SoutheastCon 2001*, pages 105–108, April 2001.

[10] Robert H. Deng, Aurel A. Lazar, and Weiguo Wang. A probabilistic approach to fault diagnosis in linear lightwave networks. *IEEE Journal on Selected Areas in Communications*, 11(9):1438–1448, December 1993.

[11] J. Fee. All-optical network technology enablers. *OFC 97*, February 1997.

[12] G. Ferraris and K. Oguchi. Management of optical networks. *24th European Conference on Optical Communication*, 1:695–696, September 1998.

[13] J. H. Franz and V. K. Jain. *Optical Communications: components and Systems.* CRC press, 2000.

[14] C. W. Geib and R. P. Goldman. Plan recognition in intrusion detection systems. *Proceeding of DISCEX'01*, 1:46–55, June 2001.

[15] Nada Golmie, Thomas D. Ndousse, and David H. Su. A differentiated optical services model for WDM networks. *IEEE Communication Magazine*, pages 68–73, February 2000.

[16] Advanced Networks Group. All-optical network security. *MIT Lincoln Laboratory*, December 1998.

[17] M. L. Jones. A carrier perspective on all-optical networks. *IEEE/LEOS All-Optical Networking: Existing and Emerging Architecture and Applications*, pages 31–32, 2002.

[18] S. Karunanithi and A. D. Friedman. Analysis of digital systems using a new measure of system diagnosis. *IEEE Trans. Comput.*, C-25:121–133, 1979.

[19] Irene Katzela, Georgios Ellinas, and Thomas E. Stern. Fault diagnosis in the linear lightwave network. *Dig. LEOS Summer Topical Meeting*, pages 41–42, 1995.

[20] Irene Katzela and Mischa Schwartz. Schemes for fault identification in communication networks. *IEEE/ACM Transactions on Networking*, 3(6):753–764, December 1995.

[21] Chung-Sheng Li and Rajiv Ramaswami. Fault detection, isolation, and open fiber control in transparent all-optical networks. *GLOBECOM '96*, 1:157 –162, 1996.

[22] Chung-Sheng Li and Rajiv Ramaswami. Automatic fault detection, isolation, and recovery in transparent all-optical networks. *IEEE Journal of Lightwave Technology*, 15:1784–1793, October 1997.

[23] Ling Li. Dynamic wavelength routing in multifiber WDM network. *Ph.D Thesis, Iowa State University*, 2000.

[24] Shoa-Kai Liu. Challenges of all-optical network evolution. *IEEE LEOS'98*, 1:182–183, December 1998.

[25] J. Lundell. A fault-tolerant approach to network security. *IEEE International Symposium on NCA 2001*, October 2001.

[26] M. Maeda. Optical network management. *Proceeding of OFC 97*, February 1997.

[27] M. W. Maeda. Management and control of transparent optical networks. *IEEE Journal on Selected Areas in Communications*, 16(7):1008–1023, September 1998.

[28] M. Marciniak. Optical transparency in next generation ip over all-optical networks. *Proceedings of 2001 3rd International Conference on Transparent Optical Networks*, pages 329–332, June 2001.

[29] A. McGuire. Management of optical transport networks. *Journal of Electronics and Communication Engineering*, 11(3):155–163, June 1999.

[30] Muriel Medard, Douglas Marquis, Richard A. Barry, and Steven G. Finn. Security issues in all-optical networks. *IEEE Network*, 11(3):42–48, May/June 1997.

[31] Muriel Medard, Douglas Marquis, and Stephen R. Chinn. Attack detection methods for all-optical networks. *Network and Distributed System Security Symposium*, 1998.

[32] M. S. M. A. Notare, A. Boukerche, and C. Westphal. Safety and security for 2000 telecommunications. *IEEE/AFCEA EUROCOMM 2000: Information Systems for Enhanced Public Safety and Security*, pages 359–363, May 2000.

[33] I. Rubin and Ling Jing. Failure protection methods for optical meshed-ring communications networks. *IEEE Journal on Selected Areas in Communications*, 18(10):1950–1960, October 2000.

[34] A. K. Somani. Sequential fault occurrence and reconfiguration in system-level diagnosis. *IEEE Trans. Comput.*, 39(12):1472–1475, December 1990.

[35] A. K. Somani. System level diagnosis: A review. *Technique Report, Dependable Computer Laboratory, Iowa State University*, 1997.

[36] A. K. Somani, V. K. Agarwal, and D. Avis. A generalized theory for system level diagnosis. *IEEE Trans. Comput.*, C-36:538–546, 1987.

[37] A. K. Somani and O. Peleg. On diagnosability of large fault sets and its applications to regular-interconnected computer systems. *IEEE Trans. Comput.*, 45(8):892–903, August 1996.

[38] S. Thomas and D. Wagner. Insecurity in atm-based passive optical networks. *ICC 2002*, 5:2803– 2805, 2002.

[39] B. J. Wilson, N. G. Stoffel, J. L. Pastor, and N. J. Post etc. Multiwavelength optical networking management and control. *Journal of Lightwave Technology*, 18(12):2038–2057, December 2000.

[40] Tao Wu and Arun K. Somani. Attack monitoring and monitor placement in all-optical network. *IEEE GBN 2001*, April 2001.

[41] Tao Wu and Arun K. Somani. Attack monitoring and localization in all-optical networks. *OptiComm'02 Proceedings*, July 2002.

[42] Tao Wu and Arun K. Somani. Necessary and sufficient condition for crosstalk attack localization in all-optical networks. *APOC'02 Proceedings*, October 2002.

[43] Tao Wu and Arun K. Somani. Attack monitoring and localization in all-optical networks. *Cluster Computing: The journal of Networks, software Tools and Applications*, 2003.

[44] Tao Wu and Arun K. Somani. Necessary and sufficient condition for k crosstalk attacks localization in all-optical netowrks. *GlobeCom'03*, 2003.

[45] Dongyun Zhou and S. Subramaniam. Survivability in optical networks. *IEEE Network*, 14(6):16–23, November 2000.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of the conducting of this research and the writing of this dissertation. First and foremost, I thank my advisor Dr. Arun K. Somani for his guidance, patience and support throughout this research and the writing of this dissertation. His unique perspective of computer networking and his mathematical discipline enhanced my understanding of many fundamental problems in fault tolerance theory. His creative instructions and critical comments made this dissertation possible. I would also like to thank my committee members for their efforts and contributions to this work. I also want to thank my parents and my wife. Without their support and encouragement, it would be impossible for me to do my research. Finally, I give thanks to the folks at the Dependable Computing and Networking Laboratory for making my study in ISU a memorable experience.